Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Estudo Exploratório sobre o Impacto acerca da Interrupção e Indisponibilidade dos Serviços de TI oferecidos pelo CPD sobre as Atividades de Pesquisa e Administrativas da UnB

Lucas Fernandes Braga Moura

Monografia apresentada como requisito parcial
para conclusão do Curso de Computação — Licenciatura

Orientador
Prof. Dr. Genaína Nunes Rodrigues

Brasília
2016

Universidade de Brasília — UnB
Instituto de Ciências Exatas
Departamento de Ciência da Computação
Curso de Computação — Licenciatura

Coordenador: Prof. Dr. Pedro Antônio Dourado Rezende

Banca examinadora composta por:

Prof. Dr. Genaína Nunes Rodrigues (Orientador) — CIC/UnB
Prof. Dr. Jorge Henrique Cabral Fernandes — CIC/UnB
Prof. Dr. André Costa Drummond — CIC/UnB

CIP — Catalogação Internacional na Publicação

Moura, Lucas Fernandes Braga.

Estudo Exploratório sobre o Impacto acerca da Interrupção e Indisponibilidade dos Serviços de TI oferecidos pelo CPD sobre as Atividades de Pesquisa e Administrativas da UnB / Lucas Fernandes Braga Moura. Brasília : UnB, 2016.
123 p. : il. ; 29,5 cm.

Monografia (Graduação) — Universidade de Brasília, Brasília, 2016.

1. análise de impacto do negócio, 2. interrupções, 3. continuidade

CDU 004.4

Endereço: Universidade de Brasília
Campus Universitário Darcy Ribeiro — Asa Norte
CEP 70910-900
Brasília–DF — Brasil

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Ciência da Computação

Estudo Exploratório sobre o Impacto acerca da Interrupção e Indisponibilidade dos Serviços de TI oferecidos pelo CPD sobre as Atividades de Pesquisa e Administrativas da UnB

Lucas Fernandes Braga Moura

Monografia apresentada como requisito parcial
para conclusão do Curso de Computação — Licenciatura

Prof. Dr. Genaína Nunes Rodrigues (Orientador)
CIC/UnB

Prof. Dr. Jorge Henrique Cabral Fernandes
CIC/UnB

Prof. Dr. André Costa Drummond
CIC/UnB

Prof. Dr. Pedro Antônio Dourado Rezende
Coordenador do Curso de Computação — Licenciatura

Brasília, 11 de julho de 2016

Dedicatória

Dedico a realização deste trabalho e finalização dessa graduação a Deus, aos meus pais, que nunca mediram esforços para me auxiliar e me acompanhar durante toda minha trajetória acadêmica e à minha namorada, Marina Ramirez, que sempre me estimulou e esteve ao meu lado nos momentos mais difíceis.

Agradecimentos

Agradeço primeiramente a Deus pela sabedoria, força e paciência que me foram concedidas duarnte a elaboração desse trabalho; a minha família por todo o suporte que me foi dado durante toda minha vida e que foi essencial para que eu alcançasse todos meus objetivos e sonhos e minha namorada, Marina Ramirez, que, durante todo esse período, esteve ao meu lado me apoiando e me dando forças para superar os obstáculos.

Ademais, não poderia esquecer de agradecer aos colaboradores do CPD que tanto me ajudaram nesse trabalho, em especial analista Luiz Gribel, o analista Reinaldo e o supervisor Domingos. Sem estes últimos, certamente, o trabalho não iria ser concretizado.

Por fim, agradeço a minha professora orientadora, professora Dra. Genaína, que, por sua vez, sempre buscou me auxiliar e ajudar, além de ter sempre acreditado no sucesso deste trabalho.

Resumo

Sistemas computacionais atualmente lidam com ambientes complexos e cada vez mais competitivos, onde as informações e as tecnologias tornaram-se vitais para todos os segmentos de negócios, uma ruptura não planejada nas operações dos serviços de tecnologia da informação pode trazer impactos significativos e muitas vezes irreversíveis. No âmbito da Universidade de Brasília, o Centro de Informática da UnB (CPD) é a unidade responsável pela infraestrutura computacional, pelo oferecimento de serviços de TI, assim como pela continuidade de negócios dos serviços e softwares que operam na Universidade de Brasília. Desse modo, esse estudo de caso tem como objetivo principal realizar uma análise de impacto, com base na Norma Complementar 06/IN01/DSIC/GSIPR e na Seção 14 da ABNT NBR ISO/IEC 27002, de possíveis interrupções dos serviços de TI oferecidos pelo CPD para as atividades de negócio críticas do Departamento de Ciência da Compuração da UnB (CIC) e do Decanato de Gestão de Pessoas (DGP). Por meio dessa análise, poderão ser direcionados esforços para implementação de um programa de Gestão de Continuidade de negócios, assegurando a disponibilidade das informações e o funcionamento adequado das atividades de pesquisa científica e administrativas das áreas escopo.

Palavras-chave: análise de impacto do negócio, interrupções, continuidade

Abstract

Currently, computational systems deal with highly complex and competitive environments, where information and technologies have become fundamental for business segments. As a result, an unplanned interruption on the activities of the information technology services may bring significant impacts. In the context of the University of Brasilia, the Informatics Center (CPD) is the area responsible for the computing infraestructure, to provide the information technology services, and to assure the business and software continuity. Thereby, the main purpose of this case study is to realize a business impact analysis (BIA), based on the Complementary Standard 06/IN01/DSIC/GSIPR and on Section 14 of ABNT NBR ISO/IEC 27002, on the critical activities performed by the Computer Science Department and the Deanery Staff Management w.r.t. interruptions on the IT services provided by the CPD at UnB. Through this analysis, it will be possible to drive efforts to implement a Business Continuity Management program, which assures the availability of the information and the proper operation of the scientific research and administrative activities.

Keywords: business impact analysis, interruptions, continuity

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

1.1 Contexto

É notório que, independente do segmento de atuação ou porte, todas as organizações estão sujeitas a riscos. Dessa forma, mesmo que a organização tenha uma gestão de riscos de segurança da informação, preparada e estruturada, haverão situações em que o inesperado pode ocorrer e medidas repressivas, corretivas e até mitigatórias podem ser insuficientes para impedir que hajam perdas significativas. Para esses eventos não previstos, é importante que a entidade adote procedimentos de gestão da continuidade do negócio.

Adicionalmente, em se tratando de um mundo globalizado, com ambientes complexos e cada vez mais competitivos, onde as informações e as tecnologias tornaram-se vitais para todos os segmentos de negócios, uma ruptura não planejada nas operações dos serviços de tecnologia da informação pode trazer impactos significativos e muitas vezes irreversíveis. Uma organização pode sofrer prejuízos financeiros e fiscais, perda da produção, exposição de imagem na mídia e perda de credibilidade junto a seus clientes e partes interessadas.

No âmbito da Universidade de Brasília, o Centro de Informática da UnB (CPD) é a unidade responsável pela infraestrutura computacional, pelo oferecimento de serviços de TI, assim como pela continuidade de negócios dos serviços e softwares que operam na Universidade de Brasília. Dessa forma, a grande maioria das atividades de negócio desenvolvidas na Universidade de Brasília, mais especificamente as atividades de Pesquisa e Administrativas, são dependentes de serviços de TI oferecidos pelo CPD.

A implementação de um processo de Gestão de Continuidade de Negócios tem como principal objetivo minimizar impactos e perdas decorrentes de falhas, possíveis desastres ou eventuais indisponibilidades sobre as atividades da organização. Ou seja, tornou-se essencial desenvolver um programa sólido de Gestão de Continuidade de Negócios e determinar o possível impacto de falhas e eventuais indisponibilidades sobre as atividades da organização, com objetivo de identificar e gerir riscos exponenciais. Em consequência, garante-se que as organizações, independentemente do segmento de negócio, possam manter a normalidade de suas atividades.

Como escopo deste trabalho foram escolhidos, além do CPD que é responsável por oferecer os serviços de TI, o CIC, Departamento de Ciência da Computação da UnB, e o DGP, Decanato de Gestão de Pessoas. A escolha do departamento e decanato supracitados se deu pelos seguintes motivos:

- **CIC:** Este foi escolhido, primeiramente, por ser o departamento responsável pelos cursos de bacharelado, engenharia e licenciatura em Computação. Adicionalmente, nota-se que o CIC está diretamente relacionado e dependente dos serviços de TI oferecidos pelo CPD, tanto para o adequado funcionamento de suas atividades administrativas quanto para os estudos e pesquisas desenvolvidos em seus diversos laboratórios por seus professores e alunos, bem como para publicação de artigos e comunicação no meio acadêmico.
- **DGP:** O Decanato de Gestão de Pessoas foi escolhido por ter uma relevância notória no funcionamento de toda a Universidade de Brasília. Essa importância decorre do fato do DGP ter como atribuições a elaboração de Políticas de Gestão de Pessoas, o desenvolvimento de atividades relativas à capacitação, à gestão de desempenho dos colaboradores, elaboração e manutenção da folha de pagamento, entre outras. Ademais, nota-se que o Decanato, a partir do entendimento inicial realizado junto ao CPD, também faz uso de diversos serviços de TI oferecidos por este para o efetivo funcionamento e desempenho de suas atividades administrativas, na grande maioria críticas até para outras atividades da universidade.

1.2 Problema

Conforme informado no contexto desse trabalho, o CPD é a unidade responsável pela infraestrutura computacional assim como pela continuidade dos serviços de TI que operam na Universidade de Brasília. Ademais, é evidente que estes serviços estejam espostos a riscos e que, fatalmente, falhas e interrupções podem ocorrer.

Dessa forma, tendo em vista que a grande maioria das atividades de negócio desenvolvidas na Universidade de Brasília, mais especificamente as atividades de Pesquisa e Administrativas, são dependentes de serviços de TI oferecidos pelo CPD, é fundamental que sejam analisados os impactos das possíveis interrupções nesses serviços de TI.

Adiconalmente, é fundamental que sejam realizados alguns questionamentos acerca da estrutura de TI da UnB e do CPD:

- Quão preparada a Universidade de Brasília está em relação ao aspecto de gestão da continuidade de negócios?
- Qual impacto para as atividades de negócio da UnB caso ocorra alguma interrupção inesperada com os serviços oferecidos pelo CPD?

1.3 Objetivos

1.3.1 Objetivo Principal

Conforme explicitado na seção anterior, tendo em vista que as atividades de negócio desenvolvidas na UnB são dependentes dos serviços de TI oferecidos pelo CPD, é fundamental que sejam analisados os impactos das possíveis interrupções nesses serviços de TI.

Dessa forma, esse estudo de caso tem como objetivo principal realizar uma análise de impacto, com base na NC06 [14], na Seção 14 da ABNT NBR ISO/IEC 27002 [11]

de possíveis interrupções dos serviços de TI oferecidos pelo CPD para as atividades de negócio críticas do Departamento de Ciência da Compuração da UnB (CIC) e do Decanato de Gestão de Pessoas (DGP).

1.3.2 Objetivos Específicos

Conforme informado anteriormente, a norma NC06 [14] e a seção 14 da norma ABNT NBR ISO/IEC 27002 [11], fornecem orientações para se realizar uma adequada análise de impacto em caso de interrupções dos serviços de TI. Primeiramente, estas orietam que Estas orientam que análise de impacto seja realizado em conjunto com os responsáveis. Posteriormente, orietam que devem ser identificadas as atividades de negócio críticas, a dependência dos serviços de TI com estas atividades críticas e os riscos que os serviços de TI estão expostos.

Dito isso, os objetivos específicos desse estudo de caso foram delimitados da seguinte forma:

- Identificação das atividades críticas do DGP e CIC
- Identificação dos riscos que os serviços de TI oferecidos pelo CPD estão expostos;
- Estabelecer uma cadeia de dependências, no formato de grafo, entre os serviços de TI do CPD e as atividades de negócio consideradas críticas.
- Realizar uma estimativa de impacto das eventuais indisponibilidades dos serviços de TI para as atividades de negócio.

1.4 Organização do Documento

O documento é iniciado com um capítulo dedicado a introdução explicitando o contexto pelo qual o trabalho está envolvido, problema evidenciado que auxiliou na motivação para desenvolvimento do trabalho, objetivo geral e objetivos específicos. Logo em seguida, no segundo capítulo, foi explicitado o referencial teórico, contendo as normas base do trabalho e melhores práticas de segurança da informação.

Posteriormente, foi elaborado um terceiro capítulo delimitando a metodologia utilizada para o desenvolvimento e obtenção dos resultados do trabalho. Resultados que, por sua vez, foram detalhados no quarto capítulo e demonstram, também, os objetivos alcançados.

Após a realização da análise dos resultados, foi elaborada uma conclusão, encontrada no quinto capítulo, contendo considerações finais do autor acerca do trabalho realizado. E, por fim, encontra-se o apêndice desse documento. Neste, podem ser vistos os questionários utilizados para entendimento das atividades críticas, bem como os questionários utilizados para mensurar o impacto das interrupções dos serviços de TI sobre as atividades de negócio.

Capítulo 2

Referencial Teórico

2.1 Segurança da Informação

Nota-se que, atualmente, a informação é um instrumento estratégico para as empresas e instituições, bem como é um recurso de vital importância nas organizações. Dessa forma, pode-se dizer que a segurança da informação aplicada adequadamente em uma empresa garante, em grande parte dos casos, a continuidade do negócios desta. Ademais, possibilita o aumento da estabilidade e permite que os ativos de tecnologia da informação estejam seguros de possíveis ameaças.

Os principios de Segurança da Informação são os conceitos que norteiam todas as ações nesta área. Diversos autores, dentre eles Laureano [30], descrevem os princípios básicos para garantir a segurança das informações:

- **Confidencialidade:** a informação somente pode ser acessada por pessoas devidamente autorizadas; é a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso ao mesmo. O aspecto mais importante deste item é garantir a identificação e autenticação das partes envolvidas.
- **Disponibilidade:** a informação ou sistema de computador deve estar disponível a quem possa acessá-la no momento em que a mesma for necessária.
- **Integridade:** a informação deve ser retornada em sua forma original no momento em que foi armazenada, garantindo a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

Sêmola et al. [30] argumentam que a segurança da informação é uma área de conhecimento dedicada na proteção dos ativos de tecnologia da informação contra acessos não autorizados, alterações indevidas ou indisponibilidade, aspectos que iriam ferir os princípios básicos citados acima. Já Mandarini [24], diz que sua principal finalidade é proteger as informações contra possíveis ameaças, a fim de garantir a continuidade do negócio, minimizar as perdas e maximizar o retorno sobre os investimentos. Adicionalmente, segundo Silva et al. [18], muito já foi realizado a fim de que a segurança da informação fosse aprimorada, apesar de não ser possível a completa erradicação dos riscos de sua utilização indevida. As autoras asseguram que a segurança da informação não deve permanecer limitada aos aspectos tecnológicos, devendo resguardar a informação em qualquer formato que se apresente. Afirmam ainda que a segurança abrange também toda

infraestrutura que permite sua utilização. Dessa forma, processos, sistemas, serviços, e a proteção devem ser proporcionais ao seu valor para organização e aos prejuízos que sua perda ou acesso indevido podem provocar.

Ademais, é evidente que grande parte das organizações possuem a informação como um insumo fundamental para o desenvolvimento de suas atividades. Por consequência, torna-se clara a necessidade estratégica de proteger essas informações a fim de garantir a continuidade e o adequado funcionamento dessas atividades.

A preocupação com segurança da informação na Administração Pública Federal vem sendo demonstrada através de diferentes instrumentos normativos. O Decreto nº 3.505/2000 institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, dizendo que um dos pressupostos básicos para essa Política de Segurança da Informação é a conscientização dos órgãos e entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco de suas vulnerabilidades [13]. O referido decreto também concede aos órgãos e entidades da Administração Pública Federal instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis. Já o Decreto nº 4.553/2002 trata da "salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal".

Outra norma que abrange aspectos importantes de segurança da informação e estabelece diretrizes para Gestão de Continuidade de Negócios nos órgãos e entidades da Administração Pública Federal é a Norma Complementar 06/IN01/DSIC/GSIPR de 2009. Esta será melhor explicitada no prosseguimento do trabalho por tratar de aspectos fundamentais que embasam a justificativa e os objetivos deste trabalho.

A ABNT [11] define segurança da informação como sendo a "preservação da confidencialidade, da integridade e da disponibilidade da informação". Nesse contexto, confidencialidade pode ser definida como a garantia de que as informações serão acessadas apenas pelas pessoas que tem autorização para acessá-las, integridade é a garantia de que as informações são corretas e completas e disponibilidade é a garantia de que as informações estarão disponíveis para serem acessadas pelas pessoas que tem autorização para vê-las quando forem necessárias. Em outras palavras, segurança da informação é a garantia de que as informações da organização serão protegidas de três maneiras: serão acessadas apenas pelas pessoas que devem ter acesso a elas, estarão corretas e completas e estarão disponíveis sempre que seus usuários precisarem, conforme a norma NBR ISO/IEC 27002:2005, ou "Código de prática para a gestão da segurança da informação" [11].

Dessa forma, ao considerar tudo que foi mencionado nesta seção, torna-se evidente a necessidade de se implementar uma adequada gestão de segurança da informação e mitigar possíveis riscos para as atividades de negócio.

2.2 Gestão da Segurança da Informação

A gestão de segurança da informação é definida como o processo de gerenciar pessoas, políticas e programas com o objetivo de assegurar a continuidade das atividades preservando o alinhamento estratégico com a missão organizacional (CAZEMIER; OVERBEEK; PETERS, 2000, apud HERATH; HERATH; BREMSER, 2010). A continuidade das ope-

rações de uma organização é obtida através da proteção das informações fundamentais ao funcionamento da organização e de todos os recursos e ativos envolvidos no seu processamento e armazenamento. Segundo Moura e Gaspary [27], a proteção da informação é conseguida através da aplicação de segurança física e lógica nas operações das empresas, e o que orienta essas práticas nas organizações são as Políticas de Segurança da Informação, que, conforme Marciano [25], abrangem recursos computacionais, recursos humanos, infraestrutura e logística.

Para direcionar o gerenciamento da segurança da informação, é fundamental que seja emitido ou aprovado um documento pela direção da organização apoiando as ações nesse sentido. Conforme a ABNT [11], a Política de Segurança da Informação é o documento que tem como objetivo mostrar a orientação e o apoio da direção da organização para a segurança da informação conforme os requisitos do negócio e de acordo com as leis e regulamentações pertinentes. Ainda segundo a ABNT, as intenções e diretrizes globais da direção da organização devem ser expressadas formalmente na Política de Segurança da Informação no sentido de fomentar a preservação da confidencialidade, da integridade e da disponibilidade da informação. Fernandes e Abreu (p.19) [20] definem Política de Segurança da Informação como a "determinação de diretrizes e ações referentes à segurança dos aplicativos, da infraestrutura, dos dados, pessoas e organizações (fornecedores e parceiros)". Em outras palavras, a Política de Segurança da Informação é um documento que deve explicitar os requisitos e orientações dos dirigentes de uma organização para determinadas ações e controles necessários para que a segurança da informação seja promovida de maneira adequada. A elaboração desse documento está em conformidade com os planos do Governo Federal, segundo Cepik et al. [16], que afirmam que a elaboração de uma Política de Segurança da Informação foi uma das metas previstas na Estratégia Geral de Tecnologia da Informação (EGTI) para o ano de 2009 para todas as instituições do Poder Executivo Federal. Para esse fim, a norma NBR ISO/IEC 27002 é um dos modelos de maior destaque, segundo Lunardi et al. [22], Moraes e Mariano [26] e Lunardi et al. [23].

2.3 Camadas Segurança da Informação

Constantemente os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvos de possíveis ameaças de vários aspectos, que visam identificar vulnerabilidades compatíveis, pontos de fraqueza capazes de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é concretizada [30].

Segundo Schneier [29], "as ameaças do mundo digital espelham as ameaças no mundo físico. Se o desfalque é uma ameaça, então o desfalque digital também é uma ameaça. Se os bancos físicos são roubados, então os bancos digitais serão roubados". Ou seja, pode-se dizer que o crime no ciberespaço abrange tudo que se pode esperar do mundo físico: roubo, extorsão, vandalismo, exploração, fraude, etc.

Conforme Sêmola [30], a gestão da segurança da informação pode ser classificada sob três pontos: físicos, humanos e tecnológicos. Os aspectos tecnológicos representam, em grande parte das vezes, a principal preocupação das organizações (redes, computadores, vírus, internet) e, por outro lado, os aspectos físicos e humanos, tão fundamentais para a segurança e continuidade do negócio quanto os aspectos tecnológicos, acabam sendo esquecidos.

No prosseguimento deste trabalho, será explicitada a classificação colocada por Adachi (2004) [12] das três camadas supracitadas: física, lógica e humana. Abaixo, segue figura que demonstra como estas se relacionam.

Figura 2.1: Camadas Segurança da Informação. [9]

2.3.1 Camada Física

A camada física pode ser definida como o ambiente em que se encontra armazenado fisicamente o *hardware* - computadores, servidores, meios de comunicação - podendo ser a sede da empresa, o escritório,ou até mesmo a fábrica. Segundo Adachi [12], "a camada física representa o ambiente em que se encontram os computadores e seus periféricos, bem como a rede de telecomunicação com seus modems, cabos e a memória física, armazenada em disquetes, fitas ou CDs".

Geralmente, empresas de pequeno e médio porte têm seus dados armazenados em servidores de rede ou estações compartilhadas. Além disso, nem sempre o acesso físico à estes equipamentos é restrito. Em grande parte das vezes, esse servidor ou estação possui acesso liberado e ilimitado à Internet, o que pode aumentar o risco de um possível incidente de segurança.

Por fim, o controle de acesso aos recursos de TI, a climatização adequada do ambiente, equipamentos para fornecimento ininterrupto de energia e firewalls são algumas maneiras que de se gerenciar a segurança desta camada.

2.3.2 Camada Lógica

A camada lógica pode ser caracterizada através da utilização de *softwares* responsáveis pela funcionalidade do hardware, pela criptografia de senhas e mensagens, pelo processamento de transações em bases de dados organizacionais, entre outros aspectos. Conforme Adachi [12], é nessa camada que se encontram as "regras, normas, protocolo de comunicação, e onde, efetivamente, ocorrem as transações e consultas.

No nível lógico, a segurança se refere ao acesso que indivíduos têm às aplicações lotadas em ambientes informatizados, sem levar em consideração o tipo da aplicação ou o tamanho do computador. Em sua grande parte, as ferramentas de controle desse nível são imperceptíveis aos olhos de pessoas externas aos ambientes de tecnologia da informação; estas só reconhecem quando têm o seu acesso barrado pelo controle de acesso [15].

Para que os riscos de segurança nessa camada sejam minimizados, é recomendado que não sejam instalados programas suspeitos no computador, que se mantenha atualizado o *software* do sistema operacional com as correções de segurança mais recentes, entre outros procedimentos adequados.

2.3.3 Camada Humana

A camada humana é constituída por todos os recursos humanos presentes em determinada organização, principalmente os que detém acesso ao ativos de tecnologia da informação, seja para utilização ou manutenção. Adicionalmente, são aspectos relevantes da referida camada: a percepção do risco: a forma como elas reagem aos incidentes de segurança que ocorrem; são usuários instruídos ou ignorantes na utilização da TI; o perigo dos intrusos maliciosos ou ingênuos; e a engenharia social [12].

É importante salientar que, das três camadas, esta camada é, notoriamente, a mais difícil de se avaliar quanto aos riscos e o gerenciamento da segurança, pelo fato de abarcar o fator humano, com características psicológicas, sócio-culturais e emocionais, que variam de forma individual [29].

Dito isso, pode-se dizer que a gestão da segurança da informação envolve mais do que gerenciar os recursos de tecnologia da informação, hardware e software, envolve, também, o gerenciamento de pessoas e processos, contudo, algumas empresas negligenciam este fator.

Dessa forma, a política de segurança da informação e a devida conscientização dos usuários acerca da utilização dos recursos de TI são algumas da formas adequadas para se gerir a segurança desta camada.

2.4 Origem das normas ABNT NBR ISO/IEC 27001/ 27002/27005

O Governo Britânico foi quem criou praticamente todas as normas internacionais, em relação a segurança da informação [20]. O primeiro padrão de segurança que deu origem a série 27000 foi o BS 7799 (British Standard). Este padrão foi dividido em duas partes: a primeira BS 7799-1 chamada código de prática para gerenciamento de segurança foi criada 1995; a segunda parte, BS 7799-2, foi criada em 2002 com objetivo de certificar as organizações a partir dos controles implementados pela primeira parte da norma.

Em 2005 as duas partes da norma foram traduzidas e publicadas pela ABNT com os nomes de NBR ISO/IEC 27002 e NBR ISO/IEC 27001, respectivamente.

Ainda em 2005, passa a existir a BS 7799-3, chamada de gestão de risco de segurança da informação [10]. A partir deste padrão, em 2008 foi criada a norma ISO/IEC 27005, que foi traduzida e publicada, passando a ser chamada NBR ISO/IEC 27005 (ABNT, 2008). O Quadro a seguir exibe a descrição das normas ISO e BS, e suas equivalências.

Em particular, a NBR ISO/IEC 27002:2005 é voltada aos controles e práticas de segurança da informação, estabelecendo uma diretriz e os princípios gerais para gestão da segurança da informação em uma organização [20].

A norma orienta as organizações na elaboração de uma Política de Segurança da Informação. Esta, por sua vez, deve orientar na constituição de normas mais específicas para o

Norma BS	Descrição da norma	Norma ISO
BS7799-1	Código de pratica para gestão da segurança da informação.	(ISO 17799) ISO/IEC 27002
BS7799-2	Técnicas e requisitos de certificação da gestão da segurança da informação.	ISO/IEC 27001
BS7799-3	Gestão de risco de segurança da informação.	ISO/IEC 27005

Figura 2.2: Normas e suas equivalências

contexto da organização e procedimentos voltados para o tratamento adequado das informações e de outros ativos organizacionais que processam ou armazenam as informações. A norma também auxilia na classificação e identificação das informações e dos outros ativos relacionados quanto à respectiva importância para organização, levando em consideração aspectos como risco de perda e de divulgação indevida. Adicionalmente, dentre os controles sugeridos pela norma, diversos são direcionados para proteção desses ativos e informações, como a análise crítica e manutenção da própria Política de Segurança da Informação, a delegação de responsabilidades relacionadas à segurança da informação e os controles de acesso físico às dependências da instituição.

Constam na norma onze seções de controles, que podem estar divididas em uma ou mais categorias de controle. A numeração dessas seções se inicia com o número cinco. Juntas, as seções de controle totalizam trinta e nove categorias principais de segurança e uma seção introdutória que aborda a análise, avaliação e tratamento de riscos. Ademais, cada seção possui um número de categorias principais de segurança da informação [11].

Em especial, a seção 14 será constantemente observada neste trabalho. Esta trata da Gestão da Continuidade do Negócio, tema chave para o estudo de caso. Dessa forma, no prosseguimento do trabalho, encontra-se melhor detalhada a referida seção.

2.5 Gestão de Continuidade de Negócios

Gestão de Continuidade de Negócios (GCN) é uma abordagem integrada que envolve a mobilização de toda a organização para gerenciar crises e recuperar as operações após a ocorrência de qualquer evento que cause uma ruptura operacional [8].

É essencial para qualquer empresa o desenvolvimento de estratégias de gestão de crises e de continuidade dos negócios. A crescente massa de informações e a grande dependência dos sistemas de computadores para a realização dos negócios, indicam que as empresas que não têm processos de gestão implementados, têm maior exposição a riscos, aos prejuízos financeiros, ao comprometimento da imagem e as ações de responsabilidade legal.

Uma pesquisa do Chartered Management Institute (CMI) [31] apontou que 91% dos entrevistados que necessitaram acionar seu Plano de Continuidade de Negócios nos últimos 12 meses concordam fortemente que possuir o plano as fizeram obter uma resposta eficaz na redução do impacto relacionado ao desastre.

No prosseguimento desta seção, será detalhada a Seção 14 da norma ISO/IEC 27002 e norma complementar 06/IN01/DSIC/GSIPR que tratam da gestão de continuidade de negócios e foram utilizadas como orientação para a realização deste trabalho.

2.5.1 Seção 14 da Norma ISO/IEC 27002

A Seção 14 da norma ISO/IEC 27002 [11] tem como objetivo principal não permitir que haja interrupção das atividades de negócio. Além disso, determina controles para proteção dos processos críticos contra a consequência de possíveis falhas ou desastres significativos e para assegurar a sua retomada em tempo hábil.

Ademais, a Seção 14 orienta que seja implementado um processo de gestão da continuidade do negócio com intuito de minimizar um impacto sobre a organização e de tornar esta capaz de recuperar possíveis perdas de ativos da informação, em caso de desastres, acidentes, falhas de equipamento ou até ações intencionais. Convém, então, que este processo sirva de orientação para identificar as atividades críticas e integrar a gestão de segurança da informação com as exigências da gestão da continuidade de negócios com outros requisitos da continuidade relativo a aspectos como operações, materiais, transporte e instalações.

É aconselhável, então, que as consequências de desastres, possíveis falhas de segurança, perda de serviços e disponibilidade dos serviços estejam sujeitas a uma análise de impacto de negócios. Ademais, para realização de uma adequada análise de impacto de negócios, é necessário que sejam identificados os eventos, riscos, que podem causar interrupções aos processos de negócio junto com o impacto de tais interrupções e suas consequências.

Por fim, é importante salientar que a referida seção traz diretrizes para tal avaliação de riscos. A seção orienta que tais avaliações sejam realizadas com total envolvimento dos responsáveis pelos processos e recursos do negócio, ou responsáveis pelos serviços de TI, além de orientar que devem ser considerados aspectos como os recursos críticos e os impactos da interrupção ao longo do tempo.

Também segundo a seção 14 da norma ISO/IEC 27002 [11], detalhada acima, convém que sejam identificados os eventos que podem causar interrupções aos processos de negócio, junto à probabilidade e impacto de tais interrupções e possíveis consequências para segurança da informação.

O item 14.1.2 da referida seção dessa norma estabelece algumas diretrizes para que tal análise de riscos seja implementada. Esse item determina que, a partir da identificação dos eventos que podem causar interrupções, é interessante que seja realizada a análise de riscos para determinar o impacto de tais interrupções.

Adicionalmente, é orientado que tais avaliações de risco sejam realizadas junto aos responsáveis pelos processos de negócio ou pelos responsáveis pelos serviços de TI. Assim, a análise dos riscos e posterior análise de impacto, caso esses riscos sejam materializados, estará melhor fundamentada e direcionada.

2.5.2 Norma Complementar 06/IN01/DSIC/GSIPR

Os problemas de vazamento de informações, ou quebra de sigilo em organizações públicas são recorrentes. Entretanto, conforme mencionado na Seção 2.1, que explicita sobre a segurança da informação, há tempos o Governo Federal brasileiro vem implementando procedimentos para gestão da Segurança da Informação com vistas a minimizar tais problemas. Grande parte destas ações está registrada em normas, decretos e Leis [19].

Desse modo, é fundamental para o prosseguimento deste trabalho que seja mencionada a Norma Complementar 06/IN01/DSIC/GSIPR [14], publicada no DOU (Diário Oficial da União) Nº 223, de 23 Nov 2009 - Seção 1. Esta estabelece diretrizes para Gestão

de Continuidade de Negócios para aspectos relacionados à segurança da informação, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

A norma define alguns conceitos importantes para o melhor entendimento da Gestão de Continuidade de Negócio. Dessa maneira, com intuito de corroborar com o tema deste trabalho, alguns conceitos foram abaixo detalhados:

- **Atividades Críticas:** atividades que devem ser executadas para garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade e permitir atingir os seus objetivos mais importantes e sensíveis ao tempo.
- **Análise de Impacto nos Negócios (AIN):** visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que afetam o desempenho dos órgãos ou entidades, bem como as técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos;
- **Ativos de informação:** os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
- **Continuidade de Negócios:** capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;
- **Desastre:** Evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;
- **Gestão de Continuidade:** processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado;
- **Incidente:** evento que tenha causado algum dano, colocado em risco, algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;
- **Programa de Gestão da Continuidade de Negócios:** processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio análises críticas, testes, treinamentos e manutenção;

Ademais aos conceitos supracitados, a norma complementar 06/IN01/DSIC/GSIPR também direciona alguns procedimentos para a adequada elaboração de um Programa

de Gestão de Contuidade de Negócios. Para este trabalho serão utilizados dois destes procedimentos:

- Definir as atividades críticas do órgão ou entidade;
- Avaliar os riscos a que estas atividades críticas estão expostas;

Dessa forma, ao final do trabalho, espera-se realizar uma análise de impacto nas atividades de negócio críticas avaliadas e detalhadas posteriormente a partir dos riscos que os departamentos e os serviços de TI do CPD estão expostos.

Capítulo 3

Metodologia do estudo de caso

Os pilares desse estudo foram as normas NC 06/IN01/DSIC/GSIPR e ISO/IEC 27002, com o objetivo de entender a interdependência entre serviços de TI e atividade de negócio, bem como de realizar uma análise de impacto a partir da interrupção dos serviços de TI sobre as atividades críticas do negócio em uma instituição do ensino superior.

Sendo assim, do ponto de vista de seus objetivos, a pesquisa é classificada como exploratória. "Um trabalho é de natureza exploratória quando envolver levantamento bibliográfico, entrevistas com pessoas que tiveram (ou tem) experiências práticas com o problema pesquisado e análise de exemplos que estimulem a compreensão. Possui ainda a finalidade básica de desenvolver, esclarecer e modificar conceitos e ideias para a formulação de abordagens posteriores" [21].

Em relação a metodologia, esta pesquisa é classificada como um estudo de caso. Segundo Wohlin, Claes, et al. [17], essa metodologia é adequada para diversos tipos de pesquisa relacionada a Engenharia de Software, visto que o objeto de estudo são, normalmente, fenômenos contemporâneos, difíceis de estudar isoladamente. O mesmo autor ainda cita que estudos de caso não geram os mesmos resultados que, por exemplo, relacionamentos casuais avaliados por experimentos, mas fornecem um profundo entendimento desse fenômeno a partir de estudos em seu contexto real .

Estas são características desta pesquisa, uma vez que foi avaliado em um contexto real e na percepção dos gestores e responsáveis de cada área avaliada: Centro de Informática da UnB (CPD), Departamento de Ciência da Computação da UnB (CIC) e Decanato de Gestão de Pessoas (DGP).

3.1 Descrição do Estudo de Caso

Conforme exposto por Wohlin, Claes, et al. [17], ao se conduzir um estudo de caso, existem cinco aspectos fundamentais que devem ser seguidos conforme explicitado na Figura 3.1

De antemão, foram realizados entendimentos das áreas escopo deste trabalho: Centro de Informática da UnB (CPD), Departamento de Ciência da Computação da UnB (CIC) e Decanato de Gestão de Pessoas (DGP). Posteriormente, dando o prosseguimento ao planejamento do trabalho, foram elaborados objetivo gerais e específicos para nortear a realização desse estudo de caso. Estes podem ser encontrados na introdução do documento.

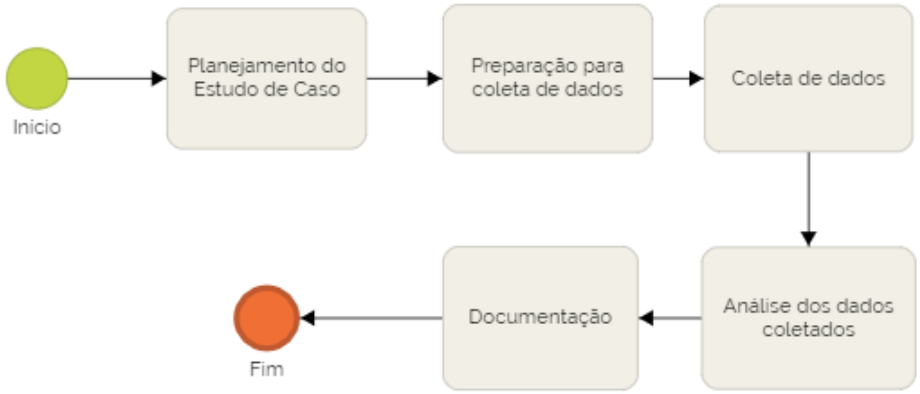

Figura 3.1: Metodologia segundo Wholin, Claes, et al.

Por fim, todas essas etapas, bem como formalização do estudo de caso, delimitadas por Wohlin, Claes, et al. [17], encontram-se melhor detalhadas no prosseguimento desse capítulo e no decorrer do documento.

3.1.1 Amostra

Em vista da dificuldade e complexidade de realização desse estudo de caso em toda universidade, o DGP - Decanato de Gestão de Pessoas e o CIC - Departamento de Ciência da Computação foram escolhidos como amostra. O primeiro foi escolhido pela notória relevância no funcionamento de toda a Universidade de Brasília, importância decorrente do fato do DGP ter como atribuições a elaboração de Políticas de Gestão de Pessoas, o desenvolvimento de atividades relativas à capacitação, à gestão de desempenho dos colaboradores, elaboração e manutenção da folha de pagamento, entre outras; e o segundo por se tratar do departamento responsável pelos cursos de bacharelado, engenharia e licenciatura em Computação, este último sendo o curso realizado pelo autor desse trabalho.

O estudo de caso foi realizado junto aos gestores das respectivas áreas:

1. CPD:
    - Coordenador do Setor de Redes;
    - Coordenador do Setor de Segurança da Informação e
    - Coordenador do Setor de Suporte Avançado.
2. CIC:
    - Coordenadores do departamento e
    - Professores do departamento.
3. DGP:
    - Decana;

- Diretor do DPAM - Diretoria de Provimento, Acompanhamento e Movimentação;
- Servidores do DPAM;
- Diretor do DAP - Diretoria de Administração de Pessoas e
- Servidores do DAP.

Pela posição e cargo, nota-se que os colaboradores tem uma ampla visão do funcionamento de suas áreas, atividades críticas, riscos à que estão expostos, pontos fortes, fraquezas e deficiências.

3.1.2 Etapas do Estudo de Caso

A pesquisa foi realizada em quatro etapas. Na primeira etapa deste trabalho, foram definidos os objetivos almejados pela pesquisa a partir da problemática que este estava exposto e também quais seriam os departamentos escopo da pesquisa. Em seguida, ainda nesta etapa, foi realizada uma pesquisa bibliográfica feita a partir das normas NC 06/IN01/DSIC/GSIPR e ISO/IEC 27002, bem como aspectos da segurança da informação e gestão da continuidade de negócios.

Na segunda etapa, foram realizadas entrevistas com os gestores das áreas de rede, segurança da informação e suporte avançado do CPD - Centro de Informática da UnB. As entrevistas tiveram como propósito o entendimento do ambiente de TI que o CPD gerencia, bem como os serviços de TI que este oferece e quais os riscos estes serviços estão expostos.

Na terceira etapa, depois de realizado o entendimento do ambiente de TI do CPD, foram realizadas entrevistas, dessa vez, com os gestores do CIC e DGP, áreas de negócio delimitadas como escopo deste estudo de caso. Para realização destas entrevistas, foi utilizado um questionário orientador, previamente elaborado, baseado em conceitos expostos nas normas NC 06/IN01/DSIC/GSIPR e ISO/IEC 27002. Adicionalmente, o principal objetivo destas entrevista foi a de conhecer as atividades de negócio críticas das duas áreas mencionadas e qual nível de dependência dessas atividades com os serviços de TI oferecidos pelo CPD. Dessa forma, foi possível a realização de uma análise qualitativa das dependências entre as principais atividades de negócio do CIC e do DGP com os serviços de TI oferecidos pelo CPD.

Na quarta etapa, depois de definidas as atividades críticas dos dois departamentos, CIC e DGP, foram realizadas aplicações de outros questionários, dessa vez, focados em avaliar o impacto de possíveis interrupções dos serviços de TI oferecidos pelo CPD para as atividades de negócio. Estes questionários foram disponibilizados para resposta de todos os professores do CIC, para a decana do DGP e os respectivos diretores da DPAM (Diretoria de Provimento, Acompanhamento e Movimentação) e DAP (Diretoria de Administração de Pessoas). Recebidas as respostas, foram realizadas análises por meio de gráficos que demonstram a estimativa de impacto nestes possíveis casos de interrupção dos serviços de TI do CPD para as atividades de negócio.

Para resposta dos questionários e posterior análise, foi utilizado a escala a seguir:

- 0 - Sem impacto;
- 1 - Impacto baixo;

- 2 - Impacto médio;
- 3 - Impacto alto;
- 4 - Impacto muito alto, crítico.

Essa escala foi embasada a partir do exemplo de análise de impacto sugerido pela empresa Gartner, Inc., especializada em pesquisas e consultoria em tecnologia da informação [5] [6].

3.2 Descrição do CPD

O Centro de Informática (CPD) é um órgão complementar da Universidade de Brasília responável pela Tecnologia da Informação e subordinado Decanato de Planejamento e Orçamento (DPO).

Este se originou a partir da criação da Universidade de Brasília, na qual se fez necessário um Centro de Informática com objetivo de instituir as atividades de caráter permanente de apoio, indispensáveis ao desenvolvimento do ensino, da pesquisa, e da extensão no que se refere ao processamento de dados.

Em 1991, foi criado o Centro de Informática, na época com a sigla CIn, com intuito de suceder ao então Centro de Processamento de Dados. A sigla permaneceu até 1993, quando, para evitar enganos corriqueiros quanto ao significado da sigla, foi retomada a abreviatura CPD.

É importante salientar que, em sua história, o CPD sempre se destacou como referência no desenvolvimento, manutenção e forncecimento de serviços de tecnologia da informação. Entre as décadas de 70 e 90, foram desenvolvidos e implementados grande parte dos sistemas coporativos que suportam as mais diversas áreas da universidade. Dentre os fatos históricos que tangem o Centro de Informática (CPD) da UnB, pode ser citado que este foi o pioneiro no desenvolvimento de sistemas de recuperação de informações em tempo real através de terminais.

Adicionalmente, com intuito de corroborar com o entendimento do Centro de Informática da UnB (CPD), abaixo estão explicitados seus objetivos estratégicos, dispostos no próprio site do centro [2]:

1. Implementar e implantar normas e padrões fundamentais nas melhores práticas de TI;
2. Promover a atualização dos softwares e infraestrutura de tecnologia da informação utilizada pela Universidade de Brasília;
3. Garantir a conectividade, qualidade e segurança dos serviços prestados;
4. Investir na capacitação dos colaboradores vinculados a área de tecnologia da informação;
5. Prover serviços de qualidade;
6. Respeitar a legislação pertinente a área de tecnologia da informação;
7. Buscar constantemente padrões de qualidade na gestão de tecnologia da informação;

8. Promover a integração, motivação e o engajamento dos servidores lotados na Unidade de tecnologia da informação;

9. Planejar, acompanhar e executar as atividades em conformidade com o Plano de Institucional - PDI.

3.2.1 Setores do CPD estudados no trabalho

O CPD, com objetivo de estar preparado e estruturado para atender adequadamente às áreas de negócio da Universidade de Brasília, se estrutura em gerências que, por sua vez, se responsabilizam pelo funcionamento suporte de determinado serviço de tecnologia da informação.

Para este estudo de caso, foram realizadas reuniões para o entendimento da gerência de redes e suporte, mais especificamente para as subáreas a seguir:

- Serviço de Suporte Avançado;
- Serviço de Segurança e Operação e
- Serviço de Administração e Segurança de Redes.

A subárea de **Serviço de Suporte Avançado** é responsável pelo suporte das máquinas, hardwares, que mantém os serviços de TI oferecidos pelo CPD. Estes equipamentos, por sua vez, suportam as atividades de negócio da UnB. Todo hardware relacionado, por exemplo, aos serviços de e-mail institucional, como servidor, ou, também, os hardwares que estão relacionados à hospedagem de sites institucionais, são de responsabilidade da referida subárea.

Outro serviço fundamental é o de realização de backup's dos dados armazenados nos bancos de dados que o CPD administra. Este serviço, por sua vez, auxilia para que a disponibilidade dos serviços de TI oferecidos esteja garantida. Adicionalmente, o referido setor realiza o monitoramento e testes de restauração dos backup's realizados, com objetivo de assegurar que estes atenderão quando necessário.

Outra subárea fundamental para este trabalho, conforme dito anteriormente, é a de **Serviço de Segurança e Operação**. Esta é responsável por gerenciar e assegurar que a sala cofre está adequada para armazenar os hardwares ali alocados e por gerenciar o *firewall* utilizado pelo CPD. Conforme detalhado no prosseguimento deste trabaho, o firewall é um recurso indispensável quando se trata da segurança de rede. Isto se justifica, devido ao fato do *firewall* se tratar de um dispositivo de uma rede computadores que tem por objetivo criar uma política de segurança a um determinado ponto de rede a partir da determinação de regras que impedem que informações indesejadas trafeguem na rede.

Por fim, a última subárea estudada foi a de **Serviço de Administração e Segurança de Redes**. Esta é responsável pelo gerenciamento e segurança do serviço de rede oferecido pelo CPD e que atende à toda infraestrutura de rede da comunidade acadêmica de alguma forma. Desde o acesso à internet sem fio até a tramitação de dados e informações na rede é realizado por meio da utilização deste serviço. Desse modo, nota-se que o serviço de rede, denominidado REDEUnB, é fundamental para as atividades acadêmicas e administrativas de servidores e docentes da universidade.

3.3 Principais serviços de TI oferecidos pelo CPD

O CPD, Centro de Informática da Universidade de Brasília, fornece diversos serviços de TI e softwares acadêmicos as demais atividades administrativas e de negócio da Universidade. Esses serviços de TI suportam e apoiam a automatização e comunicação de atividades de negócio da instituição e são fundamentais para que os objetivos de cada departamento, secretaria e área da UnB sejam alcançados de forma satisifatória.

Abaixo estão listados alguns dos principais serviços prestados pelo Centro [2] que serão melhor detalhados posteriormente.

- Disponibilização, desenvolvimento e manutenção de softwares para automação dos processos de negócios acadêmicos.
- Disponibilização, desenvolvimento e manutenção de sites de caráter institucional.
- Disponibilização e manutenção de serviço de correio eletrônico de caráter institucional.
- Disponibilização e manutenção de serviço de acesso à internet.
- Manutenção da segurança dos dados que trafegam na REDEUnB.
- Suporte técnico aos usuários de TI na instituição.

Estes serviços serão melhor detalhados nas subseções seguintes, dando destaque para os serviços de REDEUnB e Internet, serviço de correio eletrônico institucional (webmail), sistemas corporativos e hospedagem de sites institucionais.

Adicionalmente, durante a realização do trabalho, foram realizadas diversas entrevistas junto aos colaboradores do CPD com intuito de identificar e avaliar os riscos que os serviços de TI oferecidos estão expostos. Posteriormente, essa avaliação irá auxiliar no desenvolvimento da cadeia de dependências entre os serviços de TI oferecidos pelo CPD e as atividades de negócio dos setores avaliados.

3.3.1 Lista de Softwares Homologados pelo CPD

Tendo em vista que grande parte dos departamentos lotados na Universidade de Brasília faz a utilização de softwares para desevolvimento de suas atividades, no apêndice desse documento são listados os softwares acadêmicos homologados que dão suporte às mais diversas atividades administrativas, bem como uma breve descrição destes e qual departamento é atendido com o respectivo software [7].

3.3.2 REDEUnB

Um dos serviços fundamentais oferecidos pelo CPD/UnB é a REDEUnB. Esse serviço tem como objetivo garantir a conectividade dos ativos de Tecnologia da Informação da Universidade, bem como de garantir o acesso à Internet aos usuários da rede.

Dessa forma, torna-se possível a troca de informações pela comunidade acadêmica, assim como o desenvolvimento de forma adequada das atividades de alunos, professores, colaboradores e público em geral da Universidade.

De acordo com o CPD e a partir de entrevistas realizadas com colaboradores do setor responsável pela rede, a REDEUnB (Rede de Dados da Universidade de Brasília) é estruturada atualmente sobre uma ampla capilaridade de fibra óptica que abrange determinadas regiões consideravelmente afastadas do campus Darcy Ribeiro, localizado na região administrativa do Plano Pilato, setor da Asa Norte, conforme figura 4.1. Essa infraestrutura atende a aproximadamente 19200 (dezenove mil e duzentos) pontos de acesso cabeados. Essa rede é alicerçada em seu backbone por 4 (quatro) robustos switches core (de núcleo) com capacidade de backplane de 9.5 Tbps, 2.56 Tbps em capacidade de switching e suporta throughput de 1920 Mpps. O backbone é composto pelos nós identificados por ICC (Instituto Central de Ciências), FT (Faculdade de Tecnologia), FINATEC (Fundação de Empreendimentos Científicos e Tecnológicos) e o CPD (Centro de Informática).

A figura 3.2 demonstra como está disposto roteamento OSPF da rede da UnB, bem como fica clara a disposição do backbone e onde seus nós identificados, conforme mencionado acima. Essa figura foi obtida junto aos colaboradores responsáveis pela área de rede do CPD da UnB e está localizada no *website* http://www.srs.unb.br/redes/redespag3.htm, cujo acesso é restrito aos usuários do CPD.

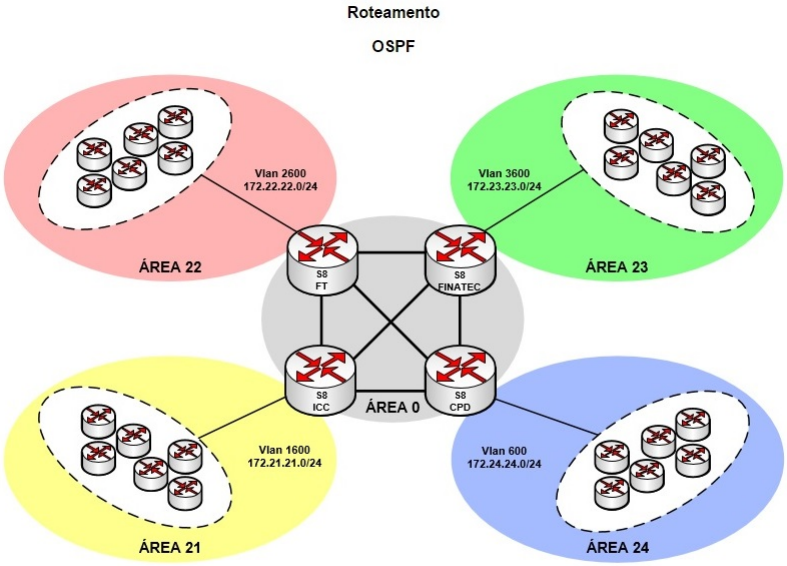

Figura 3.2: Roteamento OSPF rede UnB. Fonte: http://www.srs.unb.br/redes/redespag3.htm

Adicionalmente, conforme a Figura 3.3, nota-se o alcance da rede e algumas das regiões e campi por ela cobertas citadas abaixo:

- Faculdade de Ceilândia - FCE;
- Núcleo de práticas jurídicas - NPJ;
- Faculdade do Gama - FGA;
- Faculdade de Planaltina - FPU;
- Hospital Veterinário na Granja do Torto - HVET;

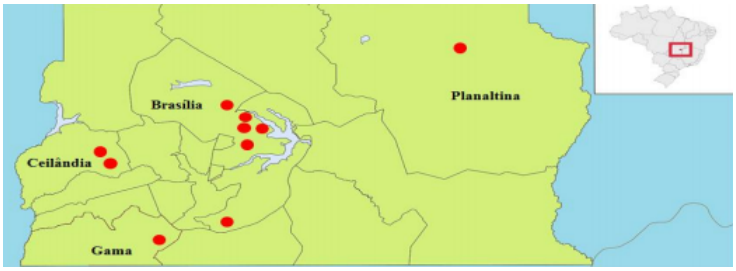

Figura 3.3: Alcançe da RedeUnB. Fonte: CPD, Rede UnB, Figura 1, http://www.cpd.unb.br/redes-e-conectividade

- Fazenda Água Limpa - FAL;
- Edifício Anápolis - SCS;
- Edifício OK - SCS;
- Estação Experimental de Biologia - EEB;
- Centro de Ensino à distância - CEAD;

Fora a REDEUnB, o CPD também fornece a rede Eduroam (Education Roaming). Este serviço é destinado principalmente para comunidade internacional de educação e pesquisa. O serviço torna possível que estudantes, pesquisadores e equipes das instituições participantes obtenham conectividade à Internet, utilizando uma conexão sem fio (wi-fi), dentro dos respectivos campi e em qualquer localidade que provenha esse serviço.

Conforme descrito pela Rede Nacional de Ensino e Pesquisa em seu site institucional [3], "o serviço Eduaroam foi lançado no Brasil em 2012. A iniciativa internacional já reúne instituições de aproximadamente 60 países, unindo diversos usuários na troca de experiências e conhecimento. Além da segurança, o eduroam tem como benefícios a sua integração à Comunidade Acadêmica Federada (CAFe), a mobilidade e a facilidade de uso."

É importante salientar que o acesso seguro e sem fio à Internet é realizado sem a necessidade de múltiplos logins e senhas. Ao ser realizado o cadastro na base do serviço, seguido da configuração do computador do usuário para conexão com a rede, é possível acessar a web em qualquer provedor de serviço do mundo.

3.3.3 UnB Webmail

Com intuito de proporcionar aos colaboradores, professores e alunos da Universidade de Brasília uma ferramenta de auxílio na comunicação entre as partes, fundamental para troca de informações e que suporta as mais variadas atividades administrativas,o CPD/UnB disponibiliza o UnB *Webmail*, ferramenta de e-mail institucional do domínio unb.br.

O UnB Webmail faz a utilização do software livre *IMP/HORDE* - ferramenta open source que se encontra em constante desenvolvimento a partir da colaboração da comunidade que a utiliza.

O acesso a ferrmaneta ocorre através de uma conexão segura, utilizando o protocolo *HTTPS*, que o torna mais prático e seguro quando da comunicação entre o computador do usuário e o servidor de e-mail da UnB. Estas informações passam por um canal criptografado de 256 bits, impedindo que outras pessoas tenham acesso às informações visualizadas pelo usuário após o seu login no sistema.

A *interface web* permite que o usuário da ferramenta tenha acesso e possa utilizar de forma adequada todas as operações possíveis relacionadas ao seu e-mail da UnB, como: envio e recebimento de mensagens; criação de pastas particulares para organizar e armazenar mensagens específicas; criação de uma lista de contatos; criação de filtros por assunto; entre outras.

Adicionalmente, por se tratar de uma ferramenta de código aberto, é recomendado que, para melhor vizualização do conteúdo, sejam utilizados navegadores também de código aberto.

Portanto, explicitado o funcionamento do e-mail e verificando que, no contexto da grande maioria das empresas, o e-mail corporativo é a principal forma de comunicação interna, é notória a criticidade e os diversos impactos negativos de eventuais interrupções da ferramenta no cotidiano corporativo.

3.3.4 Hospedagem de Site Institucional

Outro serviço de extrema importância fornecido pelo CPD/UnB é a hospedagem de sites institucionais.

Nota-se que grande parte do público universítário, para não mencionar a totalidade, faz a utilização dos serviços de Internet, bem como buscam utilizar dessa ferramenta para cumprimento de seus mais diversos objetivos. Com isso, os sites institucionais se tornam cada vez mais utilizados pelos departamentos da universidade para divulgação de suas atividades. Dessa forma, torna-se clara a relevância do serviço de hospedagem destes sites institucionais para as atividades de negócio da UnB.

Adicionalmente ao prórprio serviço de hospedagem, são disponibilizados modelos de *templates* para customização do site e orientação para utilização da ferramenta *JOOMLA*,software de gestão de conteúdo, de códido aberto, que permite a criação de sites de forma customizável e de fácil manutenção [28].

Conforme disposto no próprio site institucional do CPD, esse serviço visa atender prioritariamente os Conselhos Superiores, Reitoria, Vice Reitoria, Decanatos, Centros, Assessorias, Secretarias, Diretorias, Órgãos complementares, Órgãos auxiliares, faculdades, institutos e departamentos da universidade.

3.3.5 SEI - Sistema Eletrônico de Informações

O Sistema Eletrônico de Informações (SEI), desenvolvido pelo Tribunal Regional Federal da 4ª Região (TRF4), é a plataforma que engloba conjunto de módulos e funcionalidades que promovem a eficiência administrativa.

Trata-se também de um sistema de gestão de processos e documentos eletrônicos, com interface amigável e práticas inovadoras de trabalho, tendo como principais características a libertação do paradigma do papel como suporte físico para documentos institucionais

e o compartilhamento do conhecimento com atualização e comunicação de novos eventos em tempo real.

O SEI foi implementado em 16 de maio de 2016 na Universidade de Brasília com principal objetivo de otimizar e modernizar as rotinas de trabalho dos colaboradores da Universidade de Brasília. A partir dessa implementação, os novos documentos serão criados e tramitados com a utilização do SEI.

Tal mudança vai reduzir drasticamente a utilização de papel na Universidade, proporcionando ganhos em eficiência, agilidade e qualidade de vida no trabalho da instituição. Adicionalmente, processos extensos poderão ser mais bem analisados por meio do recurso de busca textual e problemas de perda de documentos por falhas no transporte ou controle da tramitação, comuns anteriormente, tendem a não ocorrer mais.

Ademais, o gerenciamento e suporte desse sistema estarão sob responsabilidade do Centro de Informática da UnB, CPD, justificando a inclusão desse sistema no escopo deste trabalho.

3.4 Descrição do Departamento de Ciência da Computação da UnB - CIC

O Departamento de Ciência da Computação da UnB (CIC) é resposável por oferecer cursos de graduação e pós-graduação na área de Tecnologia da Informação na Universidade de Brasília [1].

Os cursos de graduação oferecidos são:

- Bacharelado em Ciência da Computação
- Engenharia de Computação
- Engenharia Mecatrônica
- Licenciatura em Computação

Já os cursos de pós-graduação podem ser divididos em:

- Pós-Graduação em Informática
- Pós-Graduação em Computação Aplicada

O Departamento de Ciência da Computação, hoje, conta com nove servidores e cinco estagiários responsáveis por auxiliar nas atividades administrativas do departamento. Também conta com quarenta e quatro professores responsáveis por ministrar as aulas dos cursos oferecidos e desenvolver pesquisas nos mais diversos temas que abrangem a Computação, como os seguintes: Análise de Redes Sociais, Banco de Dados, Bioinformática, Computação Gráfica, Computação Paralela, Computação Sônica, Computação Ubíqua, Compressão de dados, Criptografia, Engenharia de Software, Foresight e Forecasting Tecnológico (Estudos de Futuro), Gestão da segurança da informação, Informática e Educação, Inteligência Artificial, Jogos Eletrônicos, Mineração de Dados, Orientação a objetos e software livre, Processamento Digital de Sinais e Imagens, Redes de Computadores/Segurança, Robótica, Teoria da Computação e Lógica Computacional, Sistemas

Distribuídos, Sistemas de Informação, Sistemas Embarcados, Sistemas Multiagentes e Visão Computacional.

Em apoio às mais diversas atividades de pesquisa supracitadas, o CIC conta com oito laboratórios de pesquisa em áreas específicas:

- **COMNET** (*Computer Networks LAB*): Pesquisas em redes sem fio, redes de sensores, redes ópticas, algoritmos distribuidos, otimização de roteamento, Internet do futuro, Análise de Tráfego, QoS, Segurança e Confiança.
- **LABID** (Laboratório de Bioinformática e Dados): Pesquisa em Bioinformática, Bancos de dados e Computação Distribuida.
- **LAICO** (Laboratório de Sistemas Integrados e Concorrentes): Pesquisas em Computação reconfigurável, Sistemas embarcados, robotica, desenvolvimento de jogos , hardware, microletrônica.
- **LAFORCE** (Laboratório de Formalismos da Computação e Experimentos em métodos Formais): Pesquisa em Teoria, Formalismos e Lógica Computacional, Modelagem Computacional e Matemática, Aplicações em Métodos Formais e Produção da Fala.
- **LARA** (Laboratório de Raciocínio Automatizado): Pesquisas em Inteligência artificial, inteligência artificial aplicada, sistemas de apoio a decisão, raciocínio probabilístico, representação do conhecimento, mineração de dados e textos, sistemas de recomendação, sistemas tutores inteligentes, ambientes computacionais de aprendizagem, sistemas para cooperação, e controle semafórico neuro-fuzzy.
- **LES** (Laboratório de Engenharia de Software): Pesquisa em engenharia de software, dependabilidade e confiabilidade de sistemas.
- **LISA** (Laboratório de Imagens, Sinais e Áudio): Processamento Digital de Sinais, Processamento de Imagens e Visão Computacional.
- **TRANSLAB** (Laboratório de Transporte Aéreo): Pesquisas em Web Inteligente (Rede Social, e segurança), Inteligente Artificial em Transporte aéreo, e Data Mining.

Além dos laboratórios citados, o CIC ainda conta com laboratórios de apóio à graduação, pós-graduação e pesquisas genéricas em computação.

Adicionalmente, o CIC ainda oferece atividades de extensão que vão muito além de atividades tradicionais de sala de aula. Atividades complementares como iniciação científica e tecnológica, programas acadêmicos, eventos científicos, além de atividades culturais e sociais. Alguns exemplos:

- **Projeto meninas na computação:** Fornece informação de qualidade às jovens em processo de escolha do curso para prosseguimento nos estudos.
- **Projeto Participar:** Software desenvolvido para auxiliar na educação de alunos excepcionais.

3.4.1 Estudo sobre as principais atividades desenvolvidas no CIC

Com intuito de avaliar as principais atividades de negócio realizada no departamento de Ciência da Computação da UnB - CIC, foram realizadas entrevistas junto aos professores responsáveis: Professora Dra. Alba Cristina Magalhães A. de Melo e Professor Dr. André Costa Drummond, chefe de departamento.

A partir do entendimento realizado, foi informado que a principal atividade realizada pelos professores do Departamento de Ciência da Computação da UnB é a pesquisa científica.

Ademais, além de avaliar quais as atividades críticas do CIC, as entrevistas também tiveram o objetivo de verificar os serviços de TI necessários para as atividades, a periodicidade da ocorrência de falhas e impacto inicial em caso de interrupção.

As questões elaboradas para melhor direcionar estas reuniões iniciais de entendimento encontram-se detalhadas no apêndice desse documento.

3.5 Descrição do Decanato de Gestão de Pessoas - DGP

O Decanato de Gestão de Pessoas - DGP da Universidade de Brasília pode ser considerado como órgão executivo responsável pela gestão de pessoas da universidade. Conforme apresentado em Ato da Reitoria Nº 1013/2015, o DGP tem como competências centrais a definição de políticas de Gestão de Pessoas; o desenvolvimento de atividades relativas à capacitação, à gestão de desempenho, à progressão na carreira; o gerenciamento da vida funcional do quadro técnico-administrativo e docente, do ingresso ao egresso; a execução de registros funcionais; a elaboração e manutenção da folha de pagamento; bem como a execução de ações de promoção e atenção à saúde, segurança e qualidade de vida do servidor.

Como metas específicas para este decanato, podem ser explicitadas as seguintes:

- Formular as políticas e diretrizes da sua área de atuação;
- Promover e gerir a execução das atividades relativas à administração; ao provimento, acompanhamento e movimentação; à capacitação, desenvolvimento e educação; à saúde, segurança e qualidade de vida no trabalho dos servidores que atuam na Universidade;
- Estabelecer normas e procedimentos necessários ao cumprimento das deliberações dos órgãos que compõem a Administração Superior concernentes à gestão de pessoas;
- Orientar as unidades acadêmicas e administrativas no cumprimento de normas internas e externas, relacionadas a atividades do DGP, e auxiliá-las na implementação dos procedimentos estabelecidos;
- Monitorar e avaliar metas e resultados da execução dos planos, programas e projetos institucionais;
- Efetuar o registro de atos e fatos, apurados como ilegais ou irregulares, e adotar as providências necessárias à responsabilização do agente, comunicando o fato à autoridade a quem o responsável esteja subordinado e ao órgão ou unidade do Sistema de Controle Interno.

Ademais, o referido Ato da Reitoria também explicita a missão, visão e valores do decanato da seguinte forma:

- **Missão:** Promover a gestão, desenvolvimento e potencialização de pessoas contribuindo para a busca permanente da excelência, saúde, segurança e qualidade de vida no trabalho.
- **Visão:** Ser padrão de excelência nacional em gestão de pessoas em Instituições Federais de Ensino Superior.
- **Valores:** Humanização nas relações de trabalho;Respeito à diversidade; Saúde, segurança e qualidade de vida; Excelência; Trabalho em equipe; Satisfação no trabalho; Democratização do acesso às informações; Ética e transparência nas ações; Compromisso institucional; Responsabilidade sócio ambiental.

3.5.1 Estudo sobre as principais atividades desenvolvidas no DGP

Com intuito de avaliar as principais atividades de negócio realizadas no Decanato de Gestão de Pessoas - DGP, inicialmente foi realizada reunião com a Decana do DGP, professora Dra. Maria Ângela Guimarães Feitosa, responsável por gerenciar e responder pelas atividades desempenhadas pelo Decanato.

Foi informado pela Sra. Maria Ângela que, pelo DGP se tratar do Decanato responsável pela Gestão dos Colaboradores da Universidade de Brasília, o Decanato lida com uma massa muito grande de informações pessoais, cadastrais e financeiras dos diversos servidores, docentes e pensionistas que estão vinculadas à UnB. Dessa forma, o DGP deve estar provido e suportado, de forma consitente e adequada, pelos serviços de TI do CPD devido à alta criticidade das atividades que esta área universidade é responsável.

Ainda segundo a referida Decana, dentre as diversas atividades que são desenvolvidas pelo DGP, destacam-se as atividades relacionadas a **elaboração e atualização da folha de pagamento** dos colaboradores da universidade e as atividades que suportam o **ingresso e remoção de colaboradores** na Universidade de Brasília.

Dessa forma, para que fosse realizado um melhor entendimento sobre essas atividades supracitadas, foi indicado pela decana que fossem realizadas novas reuniões junto aos diretores das respectivas áreas responsáveis: DPAM - Diretoria de Provimento, Acompanhamento e Movimentação para o processo de ingresso de colabores e DAP - Diretoria de Administração de Pessoas para atividades relacionadas a elaboração e atualização da folha de pagamento.

As questões elaboradas para melhor direcionar estas entrevistas iniciais de entendimento encontram-se detalhadas no apêndice desse documento. Dessa maneira, tornou-se possível a coleta de informações sobre quais serviços de TI oferecidos pelo CPD estão relacionados com os processos das duas diretorias do DGP delimitadas.

Capítulo 4

Resultados

4.1 Riscos que podem impactar os serviços oferecidos pelo CPD

4.1.1 Riscos que podem impactar a REDEUnB

Foi identificado que o serviço de REDEUnB está diretamente relacionada com o fornecimento de energia, cuja responsabilidade é da Prefeitura da UnB. Por exemplo, para que os pontos de acesso, que proporcionam o serviço de rede sem fio aos usuários da comunidade acadêmica, funcionem adequadamente, é necessário que haja o mínimo de energia elétrica disponível. Isso ocorre, devido à utilização de tecnologia Power over Ethernet (PoE) que permite a transmissão de energia elétrica juntamente com os dados transmitidos na rede para um dispositivo remoto através de um cabo de rede. Outro fator importante que deve ser reiterado é que a interrupção do fornecimento de energia elétrica pode causar impactos fortemente negativos no serviço de rede cabeada, como por exemplo a queima de portas de switch ou até mesmo equipamentos inteiros.

Dessa forma, caso haja uma interrupção no fornecimento de energia elétrica e ocorra uma falha nos geradores, o serviço de rede fornecido pelo CPD é totalmente comprometido, ocasionando na indisponibilidade do serviço. Tal indisponibilidade impactaria em média 6.500 acessos diários que são realizados simultaneamente.

Para corroborar essa informação, segue Figura 4.1 que explicita a quantidade de acessos diários aos serviços de rede oferecidos pelo CPD. Nota-se pela figura, extraída no dia 25/05/2016 junto aos servidores da área de rede do CPD e fazendo referência desde o dia 25/04/2016 à 25/05/2016, que em um dia a quantidade de acessos à rede pode ultrapassar dez mil. Outro fator importante que deve ser mencionado é notória diferença quantitativa dos acessos que ocorrem durante a semana em relação aos fins de semana, acompanhando certamente os dias letivos.

Para melhor analisar a Figura 4.1, deve-se considerar a numeração das semanas pelo padrão americano [4].

Ainda com relação aos acessos simultâneos ao serviço de rede oferecido pelo CPD, segue Figura 4.2 obtida junto aos colaboradores da subárea de Serviço de Administração e Segurança de Redes que, por sua vez, demonstra quais os horários este serviço é mais utilizado. Essa informação é importante tendo em vista que, caso haja uma interrupção neste serviço às 9 horas da manhã, por exemplo, aproximadamente 6.260 usuários serão

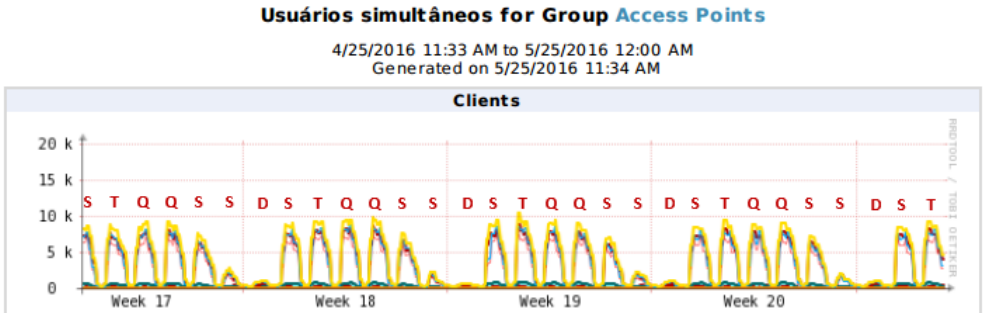

Figura 4.1: Acessos simultâneos aos seriços de Rede oferecidos pelo CPD. Fonte: imagem obtida junto aos colaboradores da área de Rede do CPD.

impactados. Caso essa interrupção ocorra às 11 horas da manhã aproximadamente 9.500 usuários serão impactados.

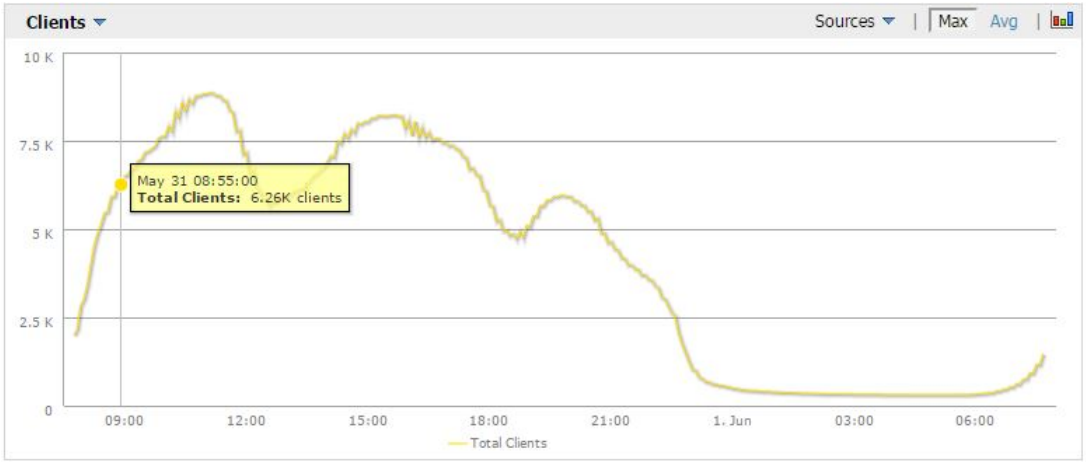

Figura 4.2: Acessos simultâneos aos seriços de Rede oferecidos pelo CPD em um período de 24 horas. Fonte: imagem obtida junto aos colaboradores da área de Rede do CPD.

Por fim, outro risco que pode comprometer substacialmente o serviço de rede ofertado pelo CPD, são possíveis depreciações na infraestrutura de cabeamento da rede, cuja responsabilidade também é da prefeitura da UnB.

4.1.2 Riscos que podem impactar o funcionamento do Firewall e, consequementemente, os serviços do CPD

Conforme conversado com colaboradores do CPD responsáveis pelo setor de Segurança da Informação, o firewall utilizado para segurança de rede é o Firewall *Next Generation* da empresa *Palo Alto Networks*. Esse dispositivo foge ao modelo convencional de endereço IP, porta e protocols, focando-se em usuários e aplicações, simplificando o gerenciamento. Adicionalmente, esse dispostivo acarreta na melhoria da produtividade de cada usuário, visto que aplicações que não fazem parte do escopo de trabalho da empresa são bloqueadas, e no aumento significativo do nível de segurança de cada usuário permitindo a geração de relatórios administrativos para o planejamento e uso da rede por cada cliente.

Contudo, é notório que, por melhor que sejam os mecanismos de segurança de uma organização, não há sistema que seja totalmente seguro, visto que vão sempre existir falhas e novas vulnerabilidades, fazendo com que haja uma preocupação constante com o sistema a ser utilizado.

4.1.3 Ocorrências que impactaram os serviços do CPD

A fim de corroborar com os entendimentos obtidos junto aos colaboradores do CPD e de analisar quantitativamente as ocorrências de indisponibilidades e interrupções dos serviços de TI oferecidos pelo CPD, solicitou-se aos gestores do Centro de Informática uma listagem de ocorrências observadas. Contudo, foi disponibilizado para realização desse estudo de caso apenas as ocorrências no período de julho à dezembro de 2015.

É importante salientar que tal relação obtida descrevia brevemente cada ocorrência e, na maioria dos casos, não explicitava o tempo que a ocorrência permaneceu vigente e em quanto tempo esta foi solucionada.

Ao ser analisada a relação, foram identificados 50 eventos que impactaram nos serviços mencionados anteriormente. As ocorrências identificadas estão relacionadas ao serviço de web-mail, serviço de rede, hospedagem de sites, aplicações oferecidas, ao firewall utilizado pelo CPD e a falhas no fornecimento energia/recebimento de energia.

A Figura 4.3, criada a partir da referida relação de ocorrências, descreve os eventos ocorridos e considerando, também, as ocorrências críticas.

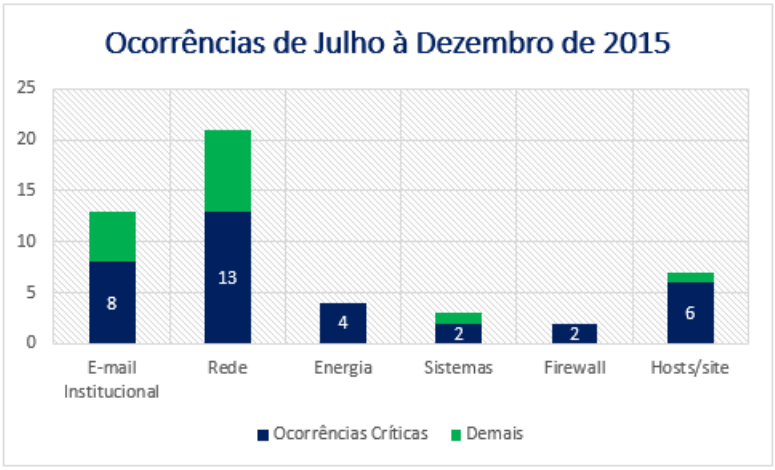

Figura 4.3: Gráfico das ocorrências no CPD.

Tornam-se, então, evidentes alguns problemas corriqueiros relacionados aos serviços oferecidos pelo CPD, decorrentes da materialização dos riscos aos quais estes serviços estão expostos, que podem impactar negativamente as atividades de negócio.

Por último, outro fator importante a ser mencionado é que, devido à restrições orçamentárias impostas ao CPD, não estão sendo mais realizados plantões aos finais de semana. Desse modo, interrupções nesse período não serão tratadas prontamente.

4.2 Cadeia de dependências entre serviços de TI do CPD e atividades de negócio

Conforme explicitado na metodologia deste trabalho, um dos objetivos traçados a ser alcançado é o de obter um grafo determinando as dependência entre as atividades de negócio das áreas escopo, CIC e DGP, e os serviços de TI oferecidos pelo CPD.

Contudo, para elaboração desse grafo de dependência, foi realizada reunião junto aos responsáveis pelas áreas escopo. Ademais, com intuito de nortear essa reunião, foi utilizado um pré-questionário localizado no apêndice B desse documento.

4.2.1 Depedências entre serviços de TI e atividades de negócio do CIC

Segundo os responsáveis pelo Departamento de Ciência da Computação da UnB, a principal atividade de negócio desenvolvida pelos professores do CIC é a pesquisa científica. Essa atividade, ainda segundo os responsáveis, depende dos seguintes serviços:

- **Internet (sem fio e cabeada):** possibilita que os professores tenham acesso adequado aos serviços de e-mail institucional da UnB, e aos demais recursos advindos da Internet, como: acesso a sites institucionais de outros pesquisadores, permite a leitura de periódicos divulgados e a realização de outras atividades inerentes ao processo de pesquisa.
- **E-mail institucional:** os artigos acadêmicos desenvolvidos devem ser enviados para publicaçao através do e-mail institucional. Essa prática é seguida pela comunidade acadêmica com intuito de assegurar a credibilidade e confiabilidade do que está sendo enviado para publicação.

Ambos serviços de tecnologia da informação são oferecidos e suportados pelo CPD da universidade. Desse modo, foram avaliados nesse trabalho e utilizados para elaboração do grafo de dependências.

Os responsáveis pelo departamento também infomaram o impacto estimado de possíveis interrupções destes serviços para a pesquisa científica e uma estimativa da periodicidade que estas ocorrem. Ademais, com intuito de melhor explicitar os possíveis impactos, segue a Tabela 4.1 que relaciona os serviços de TI mencionados, os impactos para a atividade de pesquisa científica e a periodicidade das interrupções.

Tabela 4.1: Impacto estimado dos serviços de TI no CIC

Serviço de TI	Impacto Estimado	Periodicidade de Falhas
E-mail Institucional	Alto	Uma vez ao mês.
Internet (sem fio e cabeada)	Alto	Três vezes ao mês.

Estes impactos foram estimados pelos professores responsáveis pelos seguintes aspectos:

- **Interrupções no e-mail institucional:** interrupções no serviço de e-mail podem acarretar em atrasos no envio de artigos acadêmicos desenvolvidos para publicação.

Isso poderia impactar negativamente na credibilidade da instituição UnB perante a comunidade acadêmica ou até impossibilitar a apresentação de alguns trabalhos de pesquisa em congressos e eventos de pesquisa. Ademais, tal perda de credibilidade pode impactar na atração de recursos financeiros e humanos fundamentais para realização de novas pesquisas. Ademais, são constantes os erros no controle de *spam* aos quais o e-mail institucional está esposto, constantes interrupções que acarretam em um estado crítico na fila de e-mail. Por fim, possíveis interrupções podem impactar negativamente a realização de backups dos e-mails enviados.

- **Interrupções na internet (sem fio e cabeada):** interrupções do serviço da REDEUnB podem afetar de forma abrupta as atividades inerentes à pesquisa acadêmica realizada pelos professores, visto que o acesso ao e-mail institucional, a sites institucionais, e a outros recursos necessários para pesquisa ocorrem por meio da Internet. Sem acesso à internet (sem fio e cabeada) é notório que os professores tornam-se incapacitados de acessar os servidores do CPD que contenham dados relevantes para pesquisas, atualizar o conteúdo de sites institucionais, acessar periódicos importantes para comunidade voltada de pesquisa acadêmica, acesso à informações sobre congressos, entre outros aspectos que serão impactados.

Adicionalmente, com intuito de corroborar com a elaboração do grafo de dependências, buscou-se descrever também como os serviços de TI são suportados e suas respectivas dependências.

segue Figura 4.4 que descreve a relação de dependências entre a atividade de pesquisa científica desenvolvida pelos professores do CIC, determinada como crítica por seus coordenadores responsáveis, e os serviços de TI oferecidos pelo CPD.

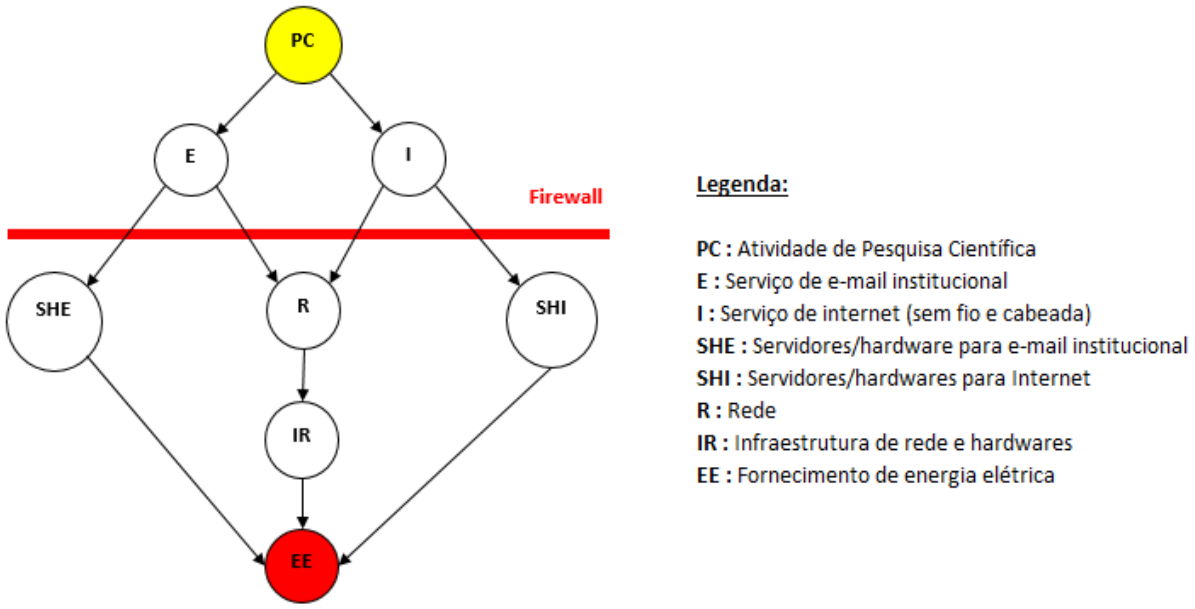

Figura 4.4: Relação de dependências entre as atividades de pesquisa científica e os serviços de TI do CPD.

A Figura 4.4 demonstra que a atividade de pesquisa científica (item PC), depende, inicialmente, dos serviços de e-mail institucional e do serviço de internet, sem fio e ca-

beada, (itens E e I), para que seja desenvolvida de forma adequada pelos professores do Departamento de Ciência da Computação.

Além disso, nota-se que estes serviços, por sua vez, dependem do correto funcionamento e da disponibilidade dos seus respectivos servidores e bancos de dados (itens SHE e SHI), bem como dependem do serviço de Rede, também disponibilizado pelo CPD.

Já o serviço de rede (item R), depende de uma infraestrutura adequada e segura (item IR), com cabeamento estruturado, além de *switches*, roteadores e *access points* funcionando adequadamente.

O *Firewall*, evidenciado pela barra em vermelho, também foi demonstrado na Figura 4.4 por se tratar do componente que aplica políticas de segurança para os serviços de TI vinculados à rede. Interrupções no *firewall* seriam de grande impacto para as atividades de negócio.

Por fim, todos os servidores e hardwares vinculados aos serviços de e-mail institucional e internet (sem fio e cabeada), bem como toda insfraestrutura de rede, dependem integralmente de um adequado fornecimento de energia elétrica (item EE) que, conforme já explicitado na descrição do serviço de rede e dentre os riscos aos quais os serviços de rede estão expostos, é de responsabilidade da prefeitura da UnB.

4.2.2 Depedências entre serviços de TI e atividades de negócio do DGP

Conforme já explicitado na metodologia, segundo a decana do DGP, dentre as diversas atividades que são desenvolvidas pelo DGP, destacam-se as atividades relacionadas a elaboração e atualização da folha de pagamento dos colaboradores da universidade e as atividades que suportam o ingresso e remoção de colaboradores na Universidade de Brasília.

Para corroborar esse entendimento, foram realizadas entrevistas junto aos diretores do DAP (Diretoria de Administração de Pessoas) e DPAM (Diretoria de Provimento, Acompanhamento e Movimentação). Segundo os diretores, as atividades de ingresso e remoção de colaboradores e elaboração e atualização da folha de pagamento dependem dos seguintes serviços de TI, respectivamente:

- **SEI (Sistema Eletrônico de Informações):** possibilita o gerenciamento da documentação referente ao ingresso, remoção e realocação de colaboradores, bem como a tramitação desses documentos.
- **SIPES:** possibilita a atualização dos dados pessoais e bancários dos colaboradores que constam na folha de pagamento da UnB. Elaborada a folha de pagamento, o sistema gera uma ficha financeira que irá auxiliar possíveis consultas de dados financeiros dos funcionários.

Ambos serviços de tecnologia da informação são oferecidos e suportados pelo CPD da universidade. Desse modo, foram avaliados nesse trabalho e utilizados para elaboração do grafo de dependências.

Os responsáveis pelas diretorias também infomaram o impacto estimado de possíveis interrupções destes serviços para as atividades críticas e uma estimativa da periodicidade que estas ocorrem. Ademais, com intuito de melhor explicitar os possíveis impactos, segue

Tabela 4.2: Impacto estimado dos serviços de TI no DGP

Serviço de TI	Impacto Estimado	Periodicidade de Falhas
Ingresso e remoção de colaboradores.	Alto	Uma vez ao mês.
Elaboração e atualização da folha de pagamento.	Alto	Três vezes ao mês.

a Tabela 4.1 que relaciona os serviços de TI mencionados, os impactos para a atividade de pesquisa científica e a periodicidade das interrupções.

Estes impactos foram estimados pelos professores responsáveis pelos seguintes aspectos:

- **Interrupções no SEI:** interrupções no Sistema Eletrônico de Informações poderia impactar no atraso do envio de documentos, documentos enviados pelo SEI podem não ser visualizados no momento adequado, entre outros.
- **Interrupções no SIPES:** interrupções no SIPES, mais especificamente no dia do fechamento da folha de pagamento, podem ser altamente críticas, visto que não será possível realizar atualizações nas informações bancárias e pessoais dos colaboradores já existentes, ou até mesmo acrescentar dados bancários de novos colaboradores que, dessa vez, irão constar na folha de pagamento.

Adicionalmente, com intuito de corroborar com a elaboração do grafo de dependências, buscou-se descrever também como os serviços de TI são suportados e suas respectivas dependências.

A Figura 4.5 descreve a relação de dependências entre a atividades críticas desenvolvidas pelos colaboradores do DGP e os serviços de TI oferecidos pelo CPD.

A figura 4.5 demonstra que as atividades elaboração e atualização da folha de pagamento e atividades relacionadas ao ingresso e remoção de colaboradores da universidade (itens FP e IC) dependem, inicialmente, dos aplicativos SIPES e SEI (itens 3 e 4), respectivamente, para que sejam desenvolvidas de forma adequada pelos colaboradores da DAP e DPAM, do DGP.

Além disso, nota-se que, da mesma forma que os serviços de e-mail institucional e de internet (sem fio e cabeada), estes aplicativos dependem do correto funcionamento e da disponibilidade dos seus respectivos servidores e bancos de dados (itens SHSi e SHSe), bem como dependem do serviço de Rede (item R), também disponibilizado pelo CPD.

Já o serviço de rede (item R) depende de uma infraestrutura de rede adequada e segura (item IR), com cabeamento estruturado, além de *switches*, roteadores e *access points* funcionando adequadamente.

O *Firewall*, demonstrado com a barra em vermelho, também foi demonstrado na Figura 4.5 por se tratar do componente que aplica políticas de segurança para os serviços de TI vinculados à rede.

Por fim, todos os servidores e hardwares vinculados aos serviços de e-mail institucional e internet (sem fio e cabeada), bem como toda insfraestrutura de rede, dependem integralmente de um adequado fornecimento de energia elétrica (item EE) que, conforme já explicitado na descrição do serviço de rede e dentre os riscos aos quais os serviços de rede estão expostos, é de responsabilidade da prefeitura da UnB.

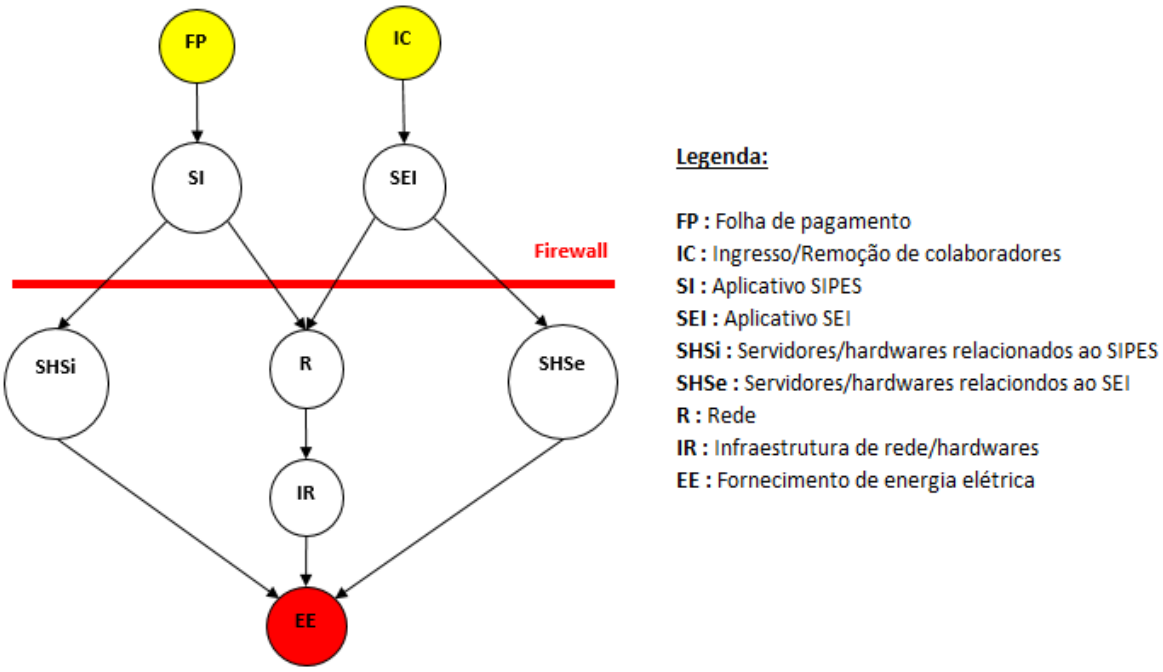

Figura 4.5: Relação de dependências entre as atividades de pesquisa científica e os serviços de TI do CPD.

4.3 Análise de Impacto a partir dos questionários enviados

De acordo com a seção 14 da norma ISO/IEC 27002, e já dito anteriormente no trabalho, é recomendado que a análise de impacto seja realizada com envolvimento dos responsáveis pelos processos e recursos do negócio, bem como devem ser considerados aspectos como a interrupção ao longo do tempo.

Dito isso e conforme explicitado em metodologia, a partir dos questionários enviados aos colaboradores do CIC e DGP, DPAM e DAP, foram realizadas análises das respostas obtidas com intuito de se obter gráficos que demonstrassem o impacto de possíveis interrupções dos serviços de TI oferecidos pelo CPD para as atividades de negócio das áreas escolhidas como escopo desse trabalho. Abaixo, encontra-se tabela demonstrando as atividades de negócios e os serviços de TI aos quais estas estão relacionadas.

Tabela 4.3: Atividades de negócio x Serviços de TI

Área	Principais atividades	Serviços de TI
CIC	Pesquisa Científica	E-mail Institucional; Internet (sem fio e cabeada).
DGP	Atualização/Manutenção de Folha de Pagamento; Ingresso/Remoção de Colaboradores.	SIPES; SEI.

É importante salientar que, para resposta dos questionários, foram dadas opções de respota entre 0 e 4, onde: 0 significa sem impacto, 1 representa um impacto baixo, 2

representa um impacto médio, 3 demonstra um impacto alto e 4 representa um impacto muito alto para as atividades de negócio.

4.3.1 Análise de Impacto - CIC

De acordo com o que já foi dito e entendido junto aos professores responsáveis pelo Departamento de Ciência da Computação da UnB, a atividade de pesquisa científica, considerada crítica por estes, é fortemente impactada em caso de interrupções nos serviços de e-mail institucional e internet, sem fio e cabeada, oferecidos pelo CPD.

Diante disso, a partir dos questionários enviados para resposta dos professores, obteu-se os seguintes gráficos que demonstram o impacto em caso de interrupção ao longo do tempo: impacto em até 1 hora ininterrupta, impacto em até 2 horas ininterruptas e impacto durante 2 a 4 horas ininterruptas. Além disso, foi questionado sobre o impacto dessas interrupções também aos finais de semana pelos mesmos intervalos de tempo. Adicionalmente, para os casos de interrupção durante os dias de semana, as questões elaboradas foram direcionadas para os horários de pico de uso da rede: de 8 às 12 horas e de 14 às 16 horas.

É importante salientar que foram enviados questionários para os 44 professores do Departamento de Ciência da Computação. Contudo, foram obtidas apenas 24 respostas. O percentual de respostas está representado na Figura 4.6.

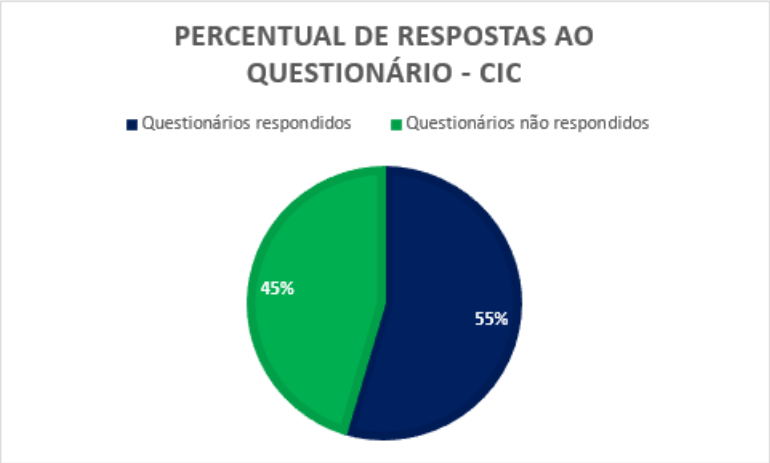

Figura 4.6: Percentual de respostas ao questionário enviado para os professores do CIC.

Tendo em vista que foi analisado o impacto para dois serviços de TI para a atividade de pesquisa científica, E-mail Institucional e Internet, foram elaborados dois gráficos, um para cada serviço de TI.

Primeiramente, segue o gráfico que demonstra o impacto em caso de interrupção do serviço de e-mail institucional para a atividade de pesquisa científica.

Neste primeiro caso, torna-se evidente que o impacto em caso de interrupção do serviço de e-mail institucional para um dia de semana por um período de até 1 hora já é considerado médio para os professores; tendo em vista que em uma escala de 0 a 4, 2 é considerado um impacto médio conforme informado no início da seção. Caso a interrupção seja de até 2 horas de forma ininterrupta, os resultados apontam que o impacto

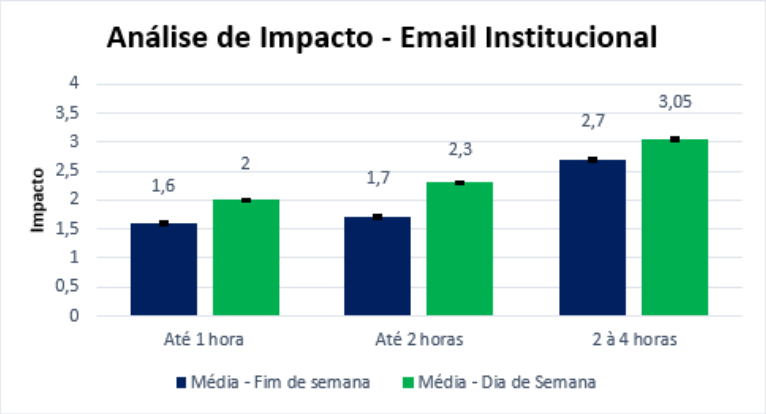

Figura 4.7: Gráfico - Análise de Impacto em Caso de Interrupção do Serviço de E-mail. Fonte: Figura elaborada pelo autor do trabalho.

ainda é médio. Contudo, é evidente que o nível de tal impacto maior do que até 1 hora de interrupção. Já entre 2 e 4 horas ininterruptas de interrupção, o impacto é considerado alto para os professores, apontando 3,05 na escala.

Aos finais de semana, por sua vez, o impacto tende a ser mais baixo, tendo em vista que não há tanto necessidade como em um dia de semana de se utilizar o serviço de e-mail. Contudo, vale salientar que entre 2 e 4 horas de interrupção do serviço de e-mail, mesmo que em um fim de semana, o impacto já está bem próximo de ser considerado alto pelos professores.

Estes resultados podem ser explicados a partir do entendimento realizado com os professores responsáveis pelo departamento. Foi informado que o impacto de possíveis interrupções no serviço de e-mail institucional é alto para as atividades de pesquisa científica.

Principalmente durante os dias de semana, a demanda de utilização do e-mail institucional pelos professores é alta. Verificamos que durante esses dias, atividades como a elaboração de artigos, submissão de artigos para publicação, entre outras atividades relacionadas à pesquisa acadêmica, são intensamente realizadas. Todas essas atividaes, por sua vez, dependem do serviço de e-mail institucional.

Adicionalmente, foi informado, também pelos professores responsáveis pelo CIC, que, aos fins de semana, constantemente o e-mail institucional é necessário.

Para corroborar a análise, foi calculada uma margem de erro, a partir do intervalo de confiança, demonstrado pelo tracejado preto no gráfico. Para os finais de semana as margens de erro encontradas foram de 0,019, 0,025 e 0,027 para até 1 hora, até 2 horas e de 2 à 4 horas, respectivamente. Para os dias de semana, as margens de erro encontradas foram de 0,022, 0,025 e 0,025 para até 1 hora, até 2 horas e de 2 à 4 horas, respectivamente.

Dando prosseguimento as análises, segue gráfico que demonstra o impacto em caso de interrupção do serviço de internet, sem fio e cabeada, para a atividade de pesquisa científica.

Como pode ser observado no gráfico, em se tratando de um dia de semana, o impacto de até 1 hora de interrupção dos serviços de internet (sem fio e cabeada) também já é considerado médio, com a taxa estando ainda um pouco acima do que o evidenciado para o serviço de e-mail. Até 2 horas o impacto está mais próximo de ser considerado

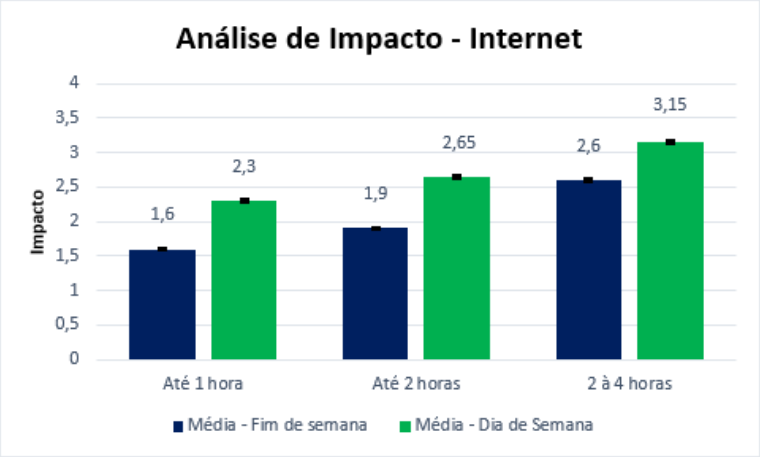

Figura 4.8: Gráfico - Análise de Impacto em Caso de Interrupção do Serviço de Internet. Fonte: Figura elaborada pelo autor do trabalho.

alto, tendo em vista que os resultados apontaram a taxa de 2,65 na escala de impacto determinada. Já de 2 a 4 horas de interupção está evidenciado que o impacto é alto para a atividade de pesquisa científica.

Ademais, seguindo o que foi observado para as interrupções do serviço de e-mail institucional, aos finais de semana, caso hajam interrupções no serviço de internet (sem fio e cabeada), o impacto tende a ser mais baixo do que nos dias de semana. Isso ocorre também pelo que já foi dito anteriormente: a utilização da internet é inevitavelmente menor em comparação do que se é utilizado durante os dias de semana.

Estes resultados também podem ser validados a partir do que foi informado pelos responsáveis pelo CIC. A partir do entendimento realizado, foi informado que o impacto é alto para as atividades de pesquisa científica em caso de interrupções do serviço de internet (sem fio e cabeada).

Durante os dias de semana, os professores tendem a utilizar bem mais o serviço de internet. Isso ocorre pelo fato da necessidade de serem realizadas consultas de periódicos, consultas de informações de congressos, submissão de artigos para publicação, análise de dados e, até mesmo, para utilizar o e-mail institucional.

Aos finais de semana, a demanda para utilização da internet se torna menor, apesar do serviço ainda ser constantemente utilizado.

Para corroborar a análise, foi calculada uma margem de erro, a partir do intervalo de confiança, demonstrado pelo tracejado preto no gráfico. Para os finais de semana as margens de erro encontradas foram de 0,018, 0,017 e 0,02 para até 1 hora, até 2 horas e de 2 à 4 horas, respectivamente. Para os dias de semana, as margens de erro encontradas foram de 0,021, 0,023 e 0,02 para até 1 hora, até 2 horas e de 2 à 4 horas, respectivamente.

Conclui-se pelos resultados apresentados na análise de impacto que os serviços de e-mail institucional e internet (sem fio e cabeada) oferecidos pelo CPD são fundamentais para realização das atividades relacionadas à pesquisa científica. Dessa forma, torna-se evidente a necessidade de que recursos sejam direcionados para o suporte desses serviços de tecnologia da informação oferecidos pelo CPD.

4.3.2 Análise de Impacto - DGP

Conforme verificado anteriomente junto à decana do DGP, e os diretores responsáveis pela Diretoria de Administração de Pessoas (DAP) e Diretoria de Provimento, Acompanhamento e Movimentação (DPAM), as principais atividades desenvolvidas pelo decanato são a elaboração e manutenção da folha de pagamento e atividades relacionadas ao ingresso e remoção de colaboradores da Universidade. Para que essas duas atividades funcionem adequadamente, são necessários os sistemas SIPES e SEI, respectivamente.

Diante disso, a partir dos questionários enviados para resposta dos colaboradores da DPAM, obteu-se o seguinte gráfico que demonstra o impacto em caso de interrupção do sistema SEI ao longo do tempo: impacto em até 1 hora ininterrupta, impacto em até 2 horas ininterruptas e impacto durante 2 a 4 horas ininterruptas. Além disso, foi questionado sobre o impacto dessas interrupções também aos finais de semana pelos mesmos intervalos de tempo.

Para os colaboradores da DPAM, foram enviados 22 questionários, número de colaboradores que atuam com o SEI para realizar as atividades voltadas para o ingresso e remoção de colaboradores. Contudo, foram obtidas 17 respostas. O percentual de respostas obtidas está representado na Figura 4.9.

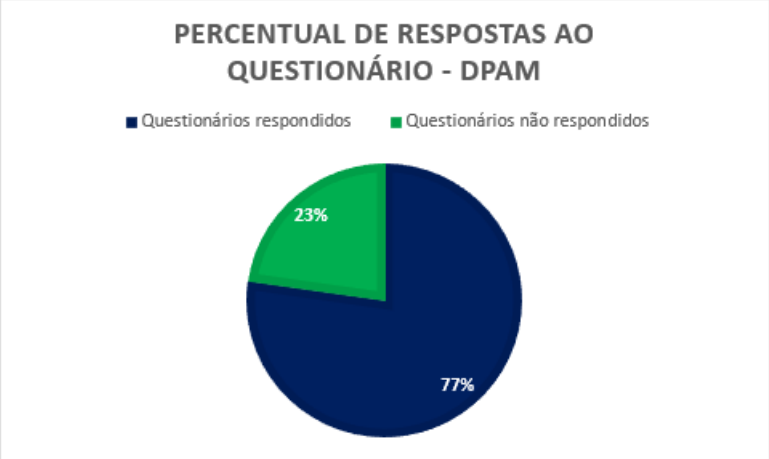

Figura 4.9: Percentual de respostas obtidas em relação aos questionários enviados aos colaboradores da DPAM

Já para os colaboradores da DAP foram enviados questionários com intuito de se obter um gráfico que demonstra o impacto em caso de interrupção do sistema SIPES ao longo do tempo. Contudo, tendo em vista que o questionamento foi direcionado para o último dia do fechamento da folha de pagamento, atividade extremamente crítica na elaboração da folha, consideramos a interrupção ao longo do tempo da seguinte forma: até 30 minutos ininterruptos, até 1 hora ininterrupta e por mais de 2 horas ininterruptas. Adicionalmente, também foi foi questionado sobre o impacto dessas interrupções aos finais de semana pelos mesmos intervalos de tempo considerados.

Para os colaboradores da DAP, foram enviados 20 questionários, número de colaboradores que atuam com o SIPES para realizar as atividades voltadas para o atualização e manutenção da folha de pagamento. Contudo, foram obtidas 18 respostas. O percentual de respostas obtidas está explicitado na Figura 4.10.

Figura 4.10: Percentual de respostas obtidas em relação aos questionários enviados aos colaboradores da DAP

Dito isso, primeiramente, segue o gráfico, Figura 4.11, que demonstra o impacto em caso de interrupção do aplicativo SEI para as atividades ingresso e remoção de colaboradores.

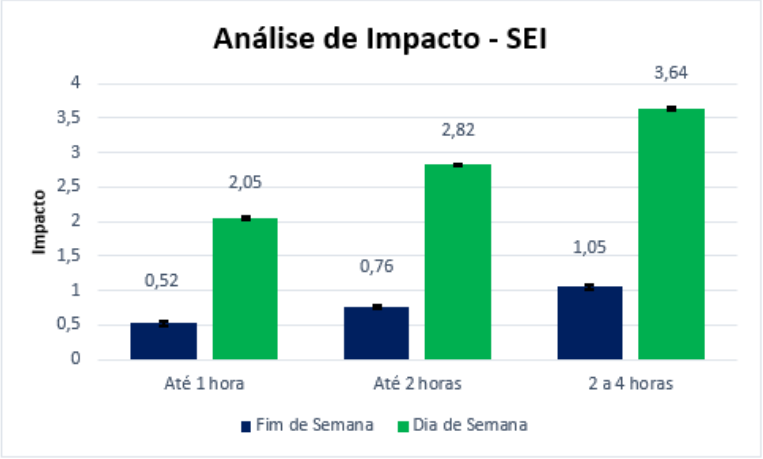

Figura 4.11: Gráfico - Análise de Impacto em Caso de Interrupção do Sistema SEI. Fonte: Figura elaborada pelo autor do trabalho.

Analisando o gráfico elaborado, é possível identificar o quão impactante uma interrupção do sistema SEI pode ser para as atividades relacionadas ao ingresso e remoção de colaboradores. Torna-se claro que até 1 hora o impacto já é considerado médio, com índice de 2,05. Caso a interrupção seja por até 2 horas o impacto já está próximo de ser considerado alto, com índice de 2,82. Já o impacto entre 2 a 4 horas é considerado muito alto, índice de 3,64, quase atigindo o limite de impacto estabelecido pela pesquisa.

Por outro lado, aos finais de semana o impacto já é considerado baixo, como o índice máximo encontrado de 1,05 entre 2 a 4 horas ininterruptas.

Estes resultados podem ser validados a partir do entendimento realizado junto ao diretor da Diretoria de Provimento, Acompanhamento e Movimentação (DPAM). Foi

informado que o impacto em caso de interrupções do sistema SEI é muito alto para as atividades voltadas para o ingresso e remoção de colaboradores.

Conforme já exposto nesse estudo de caso, a tramitação de todos os documentos utilizados na Universidade ocorreram por meio do SEI (Sistema Eletrônico de Informações). Ademais, foi informado que as atividades relacionadas ao ingresso e remoção de colaboradores da universidade dependem fundamentalmente desse sistema e estas são executadas mais intensamente durante os dias de semana.

Já aos finais de semana, pelo fato da necessidade de se utilizar o sistema ser mínima, o impacto em caso de interrupção desse serviço tende a ser baixo.

Para corroborar a análise, foi calculada uma margem de erro, a partir do intervalo de confiança, demonstrado pelo tracejado preto no gráfico. Para os finais de semana as margens de erro encontradas foram de 0,03, 0,028 e 0,028 para até 1 hora, até 2 horas e de 2 à 4 horas, respectivamente. Para os dias de semana, as margens de erro encontradas foram de 0,02, 0,021 e 0,02 para até 1 hora, até 2 horas e de 2 à 4 horas, respectivamente.

Em continuidade, segue gráfico que demonstra o impacto em caso de interrupção do sistema SIPES para a atividade de elaboração e atualização da folha de pagamento dos colaboradores da universidade.

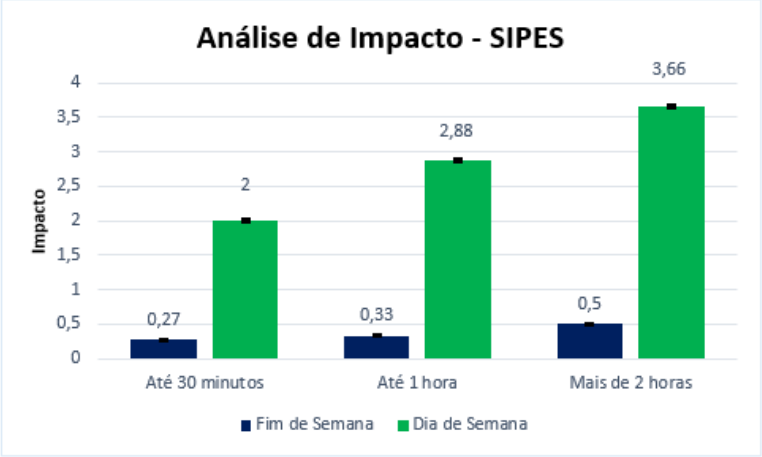

Figura 4.12: Gráfico - Análise de Impacto em Caso de Interrupção do Sistema SIPES. Fonte: Figura elaborada pelo autor do trabalho.

Conforme identificado no gráfico, É possível indentificar que, caso hajam interrupções no aplicativo SIPES durante o fechamento da folha de pagamento por até 30 minutos, o impacto é considerado médio, com índice 2, mesmo se tratando de um curto período de tempo. Caso a interrupção seja por até 1 hora, o impacto já considerado próximo de alto, tendo em vista que o índice identificado é de 2,88. Já por mais de 2 horas, o impacto sobre as atividades de elaboração e manutenção da folha de pagamento, índice de 3,66, se aproxima do nível mais alto de impacto direcionado pela pesquisa.

Em contrapartida, pode-se observar que o impacto aos finais de semana em caso de interrupção do aplicativo SIPES é muito baixo. O índice mais alto identificado foi o de 0,5, considerado um impacto muito baixo.

Estes resultados também podem ser validados por meio do entendimento realizado junto à diretora da Diretoria de Administração de Pessoas (DAP), vinculada ao DGP.

Foi informado que o impacto em caso de interrupção do SIPES no último dia do fechamento contábil é extramamente alto. Isso pode ser justificado pelo fato do último dia de fechamento da contabilidade ser direcionado para consolidação de todas as informações contábeis do período e finalização da elaboração da folha de pagamento. Dessa forma, uma interrupção, mesmo que por um período curto de tempo, pode impactar de forma muito negativa para as operações da diretoria.

Contudo, aos finais de semana, por não haver demanda de utilização do SIPES, salvo em casos excepcionais, falhas no sistema representam um impacto muito baixo para as atividades de atualização e manutenção da folha de pagamento.

Para corroborar a análise, foi calculada uma margem de erro, a partir do intervalo de confiança, demonstrado pelo tracejado preto no gráfico. Para os finais de semana as margens de erro encontradas foram de 0,01, 0,011 e 0,013 para até 1 hora, até 2 horas e de 2 à 4 horas, respectivamente. Para os dias de semana, as margens de erro encontradas foram de 0,021, 0,02 e 0,02 para até 1 hora, até 2 horas e de 2 à 4 horas, respectivamente.

Conclui-se pelos resultados apresentados na análise de impacto que os aplicativos SEI e SIPES oferecidos e suportados pelo CPD são fundamentais para realização das atividades relacionadas ao ingresso e remoção de colaboradores e atualização e manutenção da folha de pagamento. Dessa forma, torna-se evidente a necessidade de que recursos sejam direcionados para o suporte desses serviços de tecnologia da informação oferecidos pelo CPD.

Capítulo 5

Conclusões

A informação é um dos ativos mais importantes do mundo moderno. O avanço das tecnologias e comunicações transformou o ciclo de vida da informação e a forma de protegê-la. A proteção desses ativos da informação, não pode ser vista como uma iniciativa isolada de TI, ou como um conjunto de ações pontuais executadas em momentos de crise. Ela deve ser parte de um sistema de gestão apoiado em pessoas, processos, tecnologias, patrocinado pela alta administração e que atenda às demandas de segurança da organização.

Independentemente do segmento de atuação ou porte, todas as organizações estão sujeitas a riscos. A materialização desses riscos pode ocasionar paradas em sistemas, falhas de operações e até indisponibilidade das informações que estes processam. Consquentemente, as atividades depedentes destes ativos de tecnologia da informação podem ser interrompidas, podendo resultar em danos e prejuízos incalculáveis para organização.

Dessa forma, garantir a continuidade e a operação da organização, independentemente de qualquer evento ou incidente, sejam eles internos ou externos, é fundamental.

Contudo, para que seja assegurada a continuidade das operações da organização, torna-se essencial a realização de uma análise de impacto dos negócios em relação aos serviços de TI utilizados.

Apesar da Universidade de Brasília estar munida de um amplo ambiente de tecnologia da informação e possuir um Centro de Informática (CPD) de excelência responsável por dar suporte aos ativos de TI, os resultados desse trabalho apontam que a incidência de falhas e interrupções nos serviços de TI oferecidos é constante. Falhas que, muitas vezes, estão relacionadas com fatores externos à alçada do Centro.

Ademais, os resultados desse estudo de caso apontam que o impacto de possíveis interrupções nos serviços de Tecnologia de informação oferecidos pelo CPD é negativamenete alto para as atividades de negócio avaliadas.

O principal objetivo desse trabalho foi realizar uma análise de impacto de possíveis interrupções nos serviços de TI para as atividades de negócio do Departamento de Ciência da Computação (CIC) e Decanato de Gestão de Pessoas (DGP). O objetivo foi alcançado por meio das diretrizes de análise sugeridas pela ABNT NBR ISSO/IEC 27002 e Norma Complementar 06/IN01/DSIC/GSIPR.

Por fim, ao final do trabalho, tornou-se evidente a necessidade de que mais recursos humanos e financeiros sejam direcionados para as atividades do CPD, tendo em vista que as atividades de negócio estão diretamente relacionadas e dependentes dos serviços de tecnologia da informação oferecidos pelo Centro de Informática.

5.1 Trabalhos Futuros

Como trabalho futuro, existe a necessidade de que seja realizado um estudo de caso que dê prosseguimento a implementação de um programa completo de Gestão de Continuidade de Negócios. Tal necessidade existe tendo em vista que a análise de impacto é apenas um passo realizado para uma adequada Gestão de Contuidade de Negócios.

Ainda seguindo a vertente da Gestão de Continuidade de Negócios, existe a necessidade da realização de um estudo de caso para avaliar a implementação de um plano de recuperação de desastres para serviços de TI do CPD.

Por fim, outro trabalho pertinente a ser mencionado é a realização de um estudo de caso com intuito de implementar um programa de gestão de incidentes de segurança da informação, conforme seção 13 da ABNT NBR ISO/IEC 27002.

Referências

[1] CIC website. http://www.cic.unb.br/. Acessado em: 2016-05-10. 22

[2] CPD serviços. http://www.cpd.unb.br/servicos. Acessado em: 2016-04-03. 16, 18

[3] Eduroam rede nacional de ensino e pesquisa. https://portal.rnp.br/web/servicos/eduroam. Acessado em: 2016-04-13. 20

[4] EPOCH CONVERTER numeração das semanas de 2016. http://www.epochconverter.com/weeks/2016. Acessado em: 2016-06-19. 26

[5] GARTNER, INC. http://www.gartner.com/technology/about.jsp. Acessado em: 2016-06-25. 16, 50

[6] GARTNER, INC. sample bia report. http://www.hci-itil.com/ITIL_v3/docs/Sample_BIA_Report.pdf. Acessado em: 2016-06-25. 16, 50

[7] Lista de Softwares Homologados do CPD. http://www.cpd.unb.br/images/Lista_Softwares_homologados_maio2015/Lista_de_Softwares_Homologados.pdf. Acessado em: 2016-04-03. 18

[8] PwC - Gestão de Continuidade de Negócios. http://www.pwc.com.br/en/gestao-de-riscos-corporativos-e-compliance/assets/folder-gestao-continuada-13.pdf. Acessado em: 2016-05-18. 9

[9] SEGURANÇA DA INFORMAÇÃO, representação da divisão da segurança em camadas. http://www.teleco.com.br/tutoriais/tutorialitil/pagina_2.asp. Accessed: 2016-06-19. vii, 7

[10] STANDARTS ISO 27001 and 27002. http://17799.standardsdirect.org/. Acessado em: 2016-04-10. 8

[11] NBR ISO ABNT. IEC 27002: 2005. *Código de Prática para a Gestão da Segurança da Informação. Associação Brasileira de Normas Técnicas*, 2005. 2, 3, 5, 6, 9, 10

[12] Tomi Adachi. Gestão de segurança em internet banking–. *São Paulo: FGV*, 2004. 7, 8

[13] BRASIL. Decreto no 3.505, de 13 de junho de 2000. 5

[14] BRASIL. Norma complementar 06/in01/dsic/gsipr, de 11 de novembro de 2009. 2, 3, 10

[15] Carlos Alberto Antônio Caruso and Flávio Deny Steffen. *Segurança em Informática e de Informações*. Senac, 1999. 7

[16] Marco Aurelio Chaves Cepik, Diego Rafael Canabarro, and Ana Júlia Possamai. A Institucionalização do SISP e a Era Digital no Brasil. *Governança de TI: transformando a administração pública no Brasil. Porto Alegre: WS, 2010. p.[37]-74*, 2010. 6

[17] Wohlin Claes, Per Runeson, Martin Host, Magnus Ohlsson, Bjorn Regnell, and Anders Wesslén. Experimentation in software engineering: an introduction., 2000. 13, 14

[18] Pilar da Silva, Denise Ranghetti, and Lilian Milnitsky Stein. Segurança da informação: uma reflexão sobre o componente humano. *Ciências & Cognição*, 10:46–53, 2007. 4

[19] Wagner Junqueira de Araujo. Leis, decretos e normas sobre gestão da segurança da informação nos órgãos da administração pública federal. *Informação & Sociedade: Estudos*, 22, 2012. 10

[20] Aguinaldo Aragon Fernandes and Vladimir Ferraz De Abreu. *Implantando a Governança de TI-: Da estratégia à Gestão de Processos e Serviços*. Brasport, 2014. 6, 8

[21] Antonio Carlos Gil. Métodos e técnicas de pesquisa social. In *Métodos e técnicas de pesquisa social*. Atlas, 2010. 13

[22] Guilherme Lerch, Pietro Cunha Dolci, João Luiz Becker, and Antônio Carlos Gastaud. Governança de TI no Brasil: uma análise dos mecanismos mais difundidos entre as empresas nacionais. 2007. 6

[23] Guilherme Lerch Lunardi, João Luiz Becker, and Antonio Carlos Gastaud Maçada. Governança de TI e suas implicações para a gestão da TI: Um estudo acerca da percepção dos executivos. *XXXIV Encontro da ANPAD–EnANPAD. Rio de Janeiro*, 2010. 6

[24] Marcos Mandarini. *Segurança corporativa estratégica*. Editora Manole Ltda, 2005. 4

[25] João Luiz Marciano and Mamede Lima-Marques. O enfoque social da segurança da informação. *Ci. Inf., Brasília*, 35(3):89–98, 2006. 6

[26] Emerson Augusto Priamo Moraes and Sandra Regina Holanda Mariano. Uma Revisão dos Modelos de Gestão em TI. In *IV Congresso Nacional de Excelência em Gestão (CNEG)*, 2008. 6

[27] Giovane César Moreira Moura and Luciano Paschoal Gaspary. Uma proposta para medição de complexidade de segurança em procedimentos de tecnologia da informação. *VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSEG)*, pages 129–142, 2008. 6

[28] Barrie North. Joomla! guia do operador. *Rio de Janeiro: Altabooks*, 2008. 21

[29] Bruce Schneier and Daniel Vieira. *Segurança. com: Segredos e mentiras sobre a proteção na vida digital*. Campus, 2001. 6, 8

[30] Marcos Sêmola. *Gestão da segurança da informação*, volume 1. Elsevier Brasil, 2003. 4, 6

[31] Patrick Woodman, Vidal Kumar, et al. A decade of living dangerously: the business continuity management report 2009. 2009. 9

Apêndice A

Lista de Softwares Homologados pelo CPD

Abaixo, segue a listagem disponibilizada no *site* do CPD da UnB com os softwares homologados. Tal listagem tem o objetivo de informar os softwares que são suportados pela equipe de Tecnologia da Informação e Comunicações (TIC) do departamento citado.

- SIBOL
  - Objetivo: Gestão do PIC - Programa de Iniciação Científica.
  - Departamento responsável: DPP
- SGI
  - Objetivo: Gestão da locação dos imóveis e administração dos condomínios da UnB.
  - Departamento responsável: SGP
- SICONV
  - Objetivo: Gestão de convênios, contratos e acordos da UnB e respectiva consulta no Portalda Transparência da UnB.
  - Departamento responsável: DAF/DPA
- SIEFI
  - objetivo: Sistema de Execução Financeira que registra e gerencia os créditos e débitos da UnB movimentados na conta única da União.
  - Departamento responsável: DAF/DCF
- SIMAR
  - Objetivo: Gestão dos almoxarifados Central, controle do almoxarifado do CME e auxiliar na Diretoria de Gestão de Materiais.
  - Departamento responsável: DAF/DCO/DRM
- SIMCON

  - Objetivo: Gestão da dotação orçamentária dos Centros de Custo para permitir requisiçãode materiais de consumo junto ao Almoxarifado Central da UnB.
  - Departamento responsável: DAF/DCF

- SceCME
  - Objetivo: Gestão de material de controle do almoxarifado da CME/PRC.
  - Departamento responsável: PRC

- SIOF
  - Objetivo: Elaboração da lista de pretendentes a ocupação de imóveis residenciais da UnB.
  - Departamento responsável: DGP/SGP

- SIPAT
  - Objetivo: Gestão do patrimônio mobiliário da UnB e das manutenções de equipamentos do CME/PRC.
  - Departamento responsável: DAF/DRM

- SITAB
  - Objetivo: Manutenção das tabelas coorporativas da UnB.
  - Departamento responsável: Manutenção das tabelas coorporativas da UnB.

- SITRAN
  - Objetivo: Controlar a alocação de veículos utilizados nas atividades acadêmicas.
  - Departamento responsável: PRC

- SMI
  - Objetivo: Armazenamento e recuperação de informações micro filmadas.
  - Departamento responsável: Arquivo Central

- SAE
  - Objetivo: Gestão da assistência estudantil
  - Departamento responsável: DAC

- SCA
  - Objetivo: Autenticação de usuários e auditoria de utilização dos sistemas corporativos.
  - Departamento responsável: CPD

- SIPES

  - Objetivo: Gestão de pessoas, contendo todos os históricos do servidor na UnB.
  - Departamento responsável: DGP

- SRHPS
  - Objetivo: Gestão dos prestadores de serviços da UnB.
  - Departamento responsável: DGP

- SIGRA
  - Objetivo: Gestão dos cursos de graduação.
  - Departamento responsável: SAA/DEG

- SIDIP
  - Objetivo: Registro de diplomas.
  - Departamento responsável: SAA/DEG

- SIEX
  - Objetivo: Gestão dos cursos de extensão.
  - Departamento responsável: SAA/DPP

- SIPPOS
  - Objetivo: Gestão dos cursos de pós-graduação.
  - Departamento responsável: SAA/DPP

Apêndice B

Questionários

B.1 Pré-questionário para entendimento incial para delimitar as atividades críticas do CIC e do DGP

Para realização da entrevista junto aos gestores do CIC e CPD, foi elaborado um questionário direcionador, previamente elaborado, baseado nas normas ISO/IEC 27002 e NC 06/IN01/DSIC/GSIPR, orientadoras deste trabalho. Dessa forma, tornou-se possível o completo entendimento das principais atividades de negócio de cada área.

Abaixo, segue o questionário elaborado para entrevistas com os professores responsáveis pelo CIC:

1. Quais são as principais atividades administrativas e acadêmicas realizadas pelos colaboradores/professores do CIC?
2. Quais serviços de TI oferecidos pelo CPD são necessários para realização destas atividades?
3. Qual o nível do impacto para as atividades acadêmicas caso haja uma falha nestes serviços oferecidos pelo CPD?
4. Qual a periodicidade de ocorrência destas falhas?

Adicionalmente, segue o questionário elaborado para entrevistas com gestores do DGP:

1. Quais são as principais atividades administrativas e acadêmicas realizadas pelos colaboradores/gestores do DGP?
2. Quais serviços de TI oferecidos pelo CPD são necessários para realização destas atividades?
3. Qual o nível do impacto para as atividades acadêmicas caso haja uma falha nestes serviços oferecidos pelo CPD?
4. Qual a periodicidade de ocorrência destas falhas?

B.2 Questionários para avaliação do impacto em caso de interrupções nos serviços de TI oferecidos pelo CPD para as atividades críticas do CIC e DGP

Após realizadas reuniões iniciais de entendimento junto aos professores gestores do Departamento de Ciência da Computação da UnB (CIC), com a decana do Decanato de Gestão de Pessoas (DGP) e respectivos diretores da Diretoria de Administração de Pessoas (DAP) e Diretoria de Provimento, Acompanhamento e Movimentação (DPAM), e determinadas as atividades críticas dos departamentos escopo deste trabalho, CIC e DGP; foram elaborados questionários, também baseados nas normas ISO/IEC 27002 e NC 06/IN01/DSIC/GSIPR, dessa vez, com objetivo de analisar o impacto de forma temporal em caso de possíveis interrupções dos serviços de TI oferecidos pelo CPD para as atividades críticas do CIC e DGP e que foram enviados para todos os colaboradores de cada áreas, todos os professores do CIC e colaboradores da DAP e DPAM, bem como para a decana do DGP.

Ademais, nas reuniões iniciais de entendimento, foram identificados quais os serviços de TI oferecidos pelo CPD estão relacionados com as atividades críticas de ambas as áreas estudadas. Dessa forma, tais serviços foram utilizados na utilização do questionário.

Por fim, e para melhor entendimento dos questionários explicitados nas subseções seguinte, seguem às possibilidades de resposta para os questionários. Por se tratar de uma análise de impacto, as respostas foram limitadas às seguintes opções:

- 0: Sem impacto para as atividades.
- 1: Impacto relativamente baixo para as atividades.
- 2: Impacto mediano para as atividades.
- 3: Impacto relativamente alto para as atividades.
- 4: Impacto muito alto, crítico para as atividades.

Essa escala foi embasada a partir do exemplo de análise de impacto sugerido pela empresa Gartner, Inc., especializada em pesquisas e consultoria em tecnologia da informação [5] [6].

B.2.1 Questionário - Análise de impacto em caso de interrupção dos serviços de TI para as atividades críticas do CIC

A seguir, encontra-se detalhado o questionário enviado para os professores do CIC com objetivo de analisar o impacto em caso de possíveis interrupções dos serviços de E-mail institucional e Internet (sem fio e cabeada) para as atividades de pesquisa acadêmica durante os dias de semana, considerando os horários de pico evienciados: 8h às 12h e de 14 às 16h, e aos fins de semana.

Perguntas relacionadas à estimativa de impacto em caso de interrupção no serviço de **e-mail institucional** oferecido pelo CPD para as atividades de pesquisa científica.

1. Qual a estimativa do impacto em caso de interrupção do serviço de e-mail institucional por até 1 hora (ininterrupta) para as atividades de pesquisa científica em um dia de semana?
2. Qual a estimativa do impacto em caso de interrupção do serviço de e-mail institucional por até 2 horas (ininterruptas) para as atividades de pesquisa científica em um dia de semana?
3. Qual a estimativa do impacto em caso de interrupção do serviço de e-mail institucional por um período de 2 a 4 horas (ininterruptas) para as atividades de pesquisa científica em um dia de semana?
4. Qual a estimativa do impacto em caso de interrupção do serviço de e-mail institucional por até 1 hora (ininterrupta) para as atividades de pesquisa científica em um fim de semana?
5. Qual a estimativa do impacto em caso de interrupção do serviço de e-mail institucional por até 2 horas (ininterruptas) para as atividades de pesquisa científica em um fim de semana?
6. Qual a estimativa do impacto em caso de interrupção do serviço de e-mail institucional por um período de 2 a 4 horas (ininterruptas) para as atividades de pesquisa científica em um fim de semana?

Perguntas relacionadas à estimativa de impacto em caso de interrupção no serviço de **Internet (sem fio e cabeada)** oferecido pelo CPD para as atividade de pesquisa científica.

1. Qual a estimativa do impacto em caso de interrupção do serviço de internet (sem fio e cabeada) por até 1 hora (ininterrupta) para as atividades de pesquisa científica em um dia de semana?
2. Qual a estimativa do impacto em caso de interrupção do serviço de internet (sem fio e cabeada) por até 2 horas (ininterruptas) para as atividades de pesquisa científica em um dia de semana?
3. Qual a estimativa do impacto em caso de interrupção do serviço de internet (sem fio e cabeada) por um período de 2 a 4 horas (ininterruptas) para as atividades de pesquisa científica em um dia de semana?
4. Qual a estimativa do impacto em caso de interrupção do serviço de internet (sem fio e cabeada) por até 1 hora (ininterrupta) para as atividades de pesquisa científica em um fim de semana?
5. Qual a estimativa do impacto em caso de interrupção do serviço de internet (sem fio e cabeada) por até 2 horas (ininterruptas) para as atividades de pesquisa científica em um fim de semana?
6. Qual a estimativa do impacto em caso de interrupção do serviço de internet (sem fio e cabeada) por um período de 2 a 4 horas (ininterruptas) para as atividades de pesquisa científica em um fim de semana?

B.2.2 Questionário - Análise de impacto em caso de interrupção dos serviços de TI para as atividades críticas do DGP

Em seguida, encontra-se detalhado abaixo o questionário enviado para os colaboradores da DAP e DPAM, bem como para decana do DGP, com objetivo de analisar o impacto em caso de possíveis interrupções dos sistemas SEI e SIPES, sistemas corporativos gerenciados e suportados pelo CPD, para as atividades administrativas desenvolvidas no DGP durante os dias de semana e aos fins de semana.

Perguntas relacionadas à estimativa de impacto em caso de interrupção no sistema **SIPES** oferecido e suportado pelo CPD para as atividades de elaboração, atualização e manutenção da folha de pagamento.

1. Qual a estimativa de impacto em caso de interrupção no SIPES por até 30 minutos (ininterruptos), em decorrência de falhas na rede ou no próprio sistema, no último dia de fechamento para as atividades relacionadas a atualização de folha de pagamento, atualização de dados bancários e pessoais de colaboradores da UnB?
2. Qual a estimativa de impacto em caso de interrupção no SIPES por até 1 hora (ininterrupta), em decorrência de falhas na rede ou no próprio sistema, no último dia de fechamento para as atividades relacionadas a atualização de folha de pagamento, atualização de dados bancários e pessoais de colaboradores da UnB?
3. Qual a estimativa de impacto em caso de interrupção no SIPES por mais de 1 hora (ininterrupta), em decorrência de falhas na rede ou no próprio sistema, no último dia de fechamento para as atividades relacionadas a atualização de folha de pagamento, atualização de dados bancários e pessoais de colaboradores da UnB?
4. Qual a estimativa de impacto em caso de interrupção no SIPES por até 30 minutos (ininterruptos), em decorrência de falhas na rede ou no próprio sistema, no fim de semana para as atividades relacionadas a atualização de folha de pagamento, atualização de dados bancários e pessoais de colaboradores da UnB?
5. Qual a estimativa de impacto em caso de interrupção no SIPES por até 1 hora (ininterrupta), em decorrência de falhas na rede ou no próprio sistema, no fim de semana para as atividades relacionadas a atualização de folha de pagamento, atualização de dados bancários e pessoais de colaboradores da UnB?
6. Qual a estimativa de impacto em caso de interrupção no SIPES por mais de 1 hora (ininterrupta), em decorrência de falhas na rede ou no próprio sistema, no fim de semana para as atividades relacionadas a atualização de folha de pagamento, atualização de dados bancários e pessoais de colaboradores da UnB?

Perguntas relacionadas à estimativa de impacto em caso de interrupção no sistema **SEI** oferecido e suportado pelo CPD para as atividades de análise e tramitação de documentos envolvendo o ingresso ou remoção de colaboradores.

1. Qual a estimativa do impacto em caso de interrupção do serviço SEI (Sistema Eletrônico de Informações) por até 1 hora (ininterrupta) para as atividades relacionadas ao ingresso/remoção de colaboradores em um dia de semana?

2. Qual a estimativa do impacto em caso de interrupção do serviço SEI (Sistema Eletrônico de Informações) por até 2 horas (ininterruptas) para as atividades relacionadas ao ingresso/remoção de colaboradores em um dia de semana?
3. Qual a estimativa do impacto em caso de interrupção do serviço SEI (Sistema Eletrônico de Informações) por um período de 2 a 4 horas (ininterruptas) para as atividades relacionadas ao ingresso/remoção de colaboradores em um dia de semana?
4. Qual a estimativa do impacto em caso de interrupção do serviço SEI (Sistema Eletrônico de Informações) por até 1 hora (ininterrupta) para as atividades relacionadas ao ingresso/remoção de colaboradores em um fim de semana?
5. Qual a estimativa do impacto em caso de interrupção do serviço SEI (Sistema Eletrônico de Informações) por até 2 horas (ininterruptas) para as atividades relacionadas ao ingresso/remoção de colaboradores em um fim de semana?
6. Qual a estimativa do impacto em caso de interrupção do serviço SEI (Sistema Eletrônico de Informações) por um período de 2 a 4 horas (ininterruptas) para as atividades relacionadas ao ingresso/remoção de colaboradores em um fim de semana?